(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2009 年 9 月 3 日(03.09.2009)

PCT

(10) 国際公開番号
WO 2009/107330 A1

(51) 国際特許分類:
G06F 21/22 (2006.01) *G06F 12/14* (2006.01)

(21) 国際出願番号: PCT/JP2009/000500

(22) 国際出願日: 2009 年 2 月 9 日(09.02.2009)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2008-043009 2008 年 2 月 25 日(25.02.2008) JP

(71) 出願人 (米国を除く全ての指定国について): パナソニック株式会社 (PANASONIC CORPORATION) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 伊藤孝幸 (ITO, Takayuki). 前田学(MAEDA, Manabu). 芳賀智之(HAGA, Tomoyuki). 高山久(TAKAYAMA, Hisashi). 松島秀樹(MATSUSHIMA, Hideki).

(74) 代理人: 中島司朗, 外(NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目２番１号淀川５番館６Ｆ Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

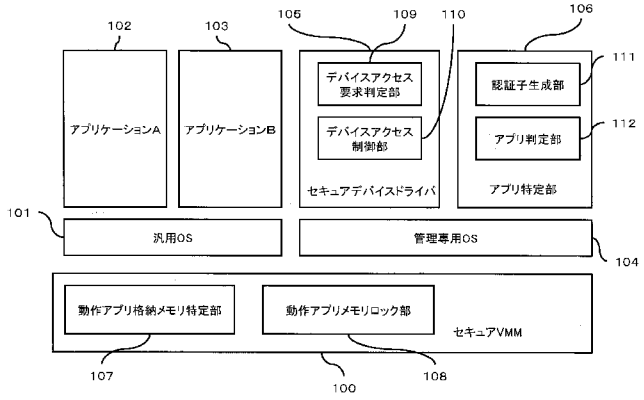
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF,

[続葉有]

(54) **Title**: INFORMATION PROCESSOR AND METHOD FOR CONTROLLING THE SAME

(54) 発明の名称: 情報処理装置及びその制御方法

[図1]



102... APPLICATION A
103... APPLICATION B
105... SECURE DEVICE DRIVER
109... DEVICE ACCESS REQUEST DETERMINING SECTION
110... DEVICE ACCESS CONTROL SECTION
111... AUTHENTICATOR GENERATING SECTION
112... APPLICATION DETERMINING SECTION
106... APPLICATION IDENTIFYING SECTION
101... UNIVERSAL OS
104... MANAGEMENT-ONLY OS
107... ACTIVE APPLICATION STORAGE MEMORY IDENTIFYING SECTION
108... ACTIVE APPLICATION MEMORY LOCK SECTION
100... SECURE VMM

(57) **Abstract**: This object aims to provide an information processor for confirming the validity to an application having actually performed a device access request. Thus, when an application (102) on a universal OS performs a processing request to a secure device driver (105), a secure VMM (100) and an application identifying section (106) on a management-only OS (104) lock the page table of the application (102) and generate a hash value with reference to the page table. The generated hash value is compared with a reference hash value to judge whether the application is correct or not.

(57) 要約: 本発明は、デバイスアクセス要求を実際に行ったアプリケーションに対して、正当性を確認する情報処理装置を提供することを目的とする。 上記目的を達成するために、本発明は、汎用ＯＳ上のアプリケーション１０２が、セキュアデバイスドライバ１０５に処理要求を行った際に、セキュアＶＭＭ１００と管理専用ＯＳ１０４上のアプリ特定部１０６が、前記アプリケーション１０２のページテーブルをロックし、前記ページテーブルを参照してハッシュ値を生成する。前記生成したハッシュ値と参照ハッシュ値とを比較して、正当なアプリケーションか否かを判定する。

WO 2009/107330 A1

CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

情報処理装置及びその制御方法

技術分野

[0001] 本発明は、所定のアプリケーションが動作する仮想マシンを管理する仮想マシンモニタを有する情報処理装置及びその制御方法に関するものである。

技術背景

[0002] 近年、民生機器では、音楽データをディジタル化して記憶装置に取り込み、音楽を楽しむということが行われるようになっている。また、音楽データの取り扱いのみならずＨｉｇｈ　Ｄｅｆｉｎｉｔｉｏｎ（ＨＤ）画像など、より表現能力が高いコンテンツの取り扱いが民生機器に求められるようになっている。

[0003] ここで、ディジタル化された音楽データや上記ＨＤ画像等は、劣化なしで複製することが可能である。そこで、著作権者の利益を保護するために、これらのコンテンツは不正な複製等から保護されて取り扱われなければならない。

[0004] そのため、これらのコンテンツは、ＣＰＲＭ（Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　Ｒｅｃｏｄｉｎｇ　Ｍｅｄｉａ）やＡＡＣＳ（Ａｄｖａｎｃｅｄ　Ａｃｃｅｓｓ　Ｃｏｎｔｅｎｔ　Ｓｙｓｔｅｍ）などの著作権保護技術で保護されている。それら、著作権保護技術では、コンテンツを暗号化することによって保護しており、それらのコンテンツをユーザが利用するには、著作権保護技術に対応する端末でデータの復号を行う必要がある。

[0005] 著作権保護技術に対応した端末では、暗号化されたコンテンツに対して復号処理を実施する暗号エンジンなどのセキュアデバイスを備えている。そのセキュアデバイスは不正な処理によって、復号が許可されていないコンテンツの復号を行わないように正しく操作される必要がある。

[0006] 前述のセキュアデバイス操作を行うプログラムが正当であるか否かを判定する技術として、改ざん検出がある（例えば、特許文献１）。

[0007] 特許文献１は、データを扱うプログラムが正当であるか否かを検出する技術であり、図１９を用いて簡単に説明を行う。図１９は、特許文献１のシーケンスを示す図である。

[0008] まず、ユーザなどの操作によって、処理が開始される（Ｓ４１０）。

[0009] 次に、プログラムが入力データに対して処理を行い、処理済み情報を出力する（Ｓ４１１）。

[0010] 次に、前述のプログラムに対して、ハッシュ関数を用いて、ハッシュ値（認証子）を作成する（Ｓ４１２）。

[0011] 次に、図示していない検証部に、前述の処理済み情報と前述のハッシュ値（認証子）とを送付し、検証部が、送付されたハッシュ値（認証子）が、予め保持しているハッシュ値と一致するか否か判定する。一致する場合には、ハッシュ値に対応するプログラムが正当であると判断する（Ｓ４１３）。

[0012] そして、処理を終了する（Ｓ４１４）。

[0013] また、端末のデバイスが扱うデータを、適切に処理する技術として、例えば特許文献２がある。図２０と図２１を用いて簡単に説明を行う。

[0014] 図２０は、特許文献２のソフトウェア構成図を示す図である。

[0015] 特許文献２のソフトウェアは、ＶＭＭ（Ｖｉｒｕａｌ Ｍａｃｈｉｎｅ Ｍｏｎｉｔｏｒ、仮想マシンモニタ）４００と、汎用ＯＳ４０１とネットワーク対応アプリ４０２と、汎用ＯＳ　ＮＩＣプロキシ４０３と、リアルタイムＯＳ４０４と、リアルタイムＮＩＣプロキシ４０５と、リアルタイムＵＤＰ／ＩＰ４０６と、ＮＩＣドライバ４０７と、から構成される。

[0016] ＶＭＭ４００は、ＯＳ仮想化機能を提供する。汎用ＯＳ４０１とリアルタイムＯＳ４０４は、ＶＭＭ４００が提供する仮想化されたハードウェア上で動作するオペレーティングシステムである。

[0017] ネットワーク対応アプリ４０２は、ネットワーク処理を行う場合には、汎用ＯＳ　ＮＩＣプロキシ４０３にネットワーク処理を依頼する。そして、汎用ＯＳ　ＮＩＣプロキシ４０３は、リアルタイムＮＩＣプロキシ４０５に処理を依頼する。そして、リアルタイムＮＩＣプロキシ４０５は、リアルタイ

ムＵＤＰ／ＩＰ４０６に処理を依頼する。リアルタイムＵＤＰ／ＩＰ４０６は、ＮＩＣドライバ４０７を利用して、図示していないネットワークインターフェースカード（ＮＩＣ、Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）を制御する。

[0018] また、リアルタイムＵＤＰ／ＩＰ４０６が、ネットワーク処理を行う場合にも、ＮＩＣドライバ４０７を利用してネットワークインターフェースカード（ＮＩＣ、Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）を制御する。

[0019] 図２１は、ネットワークインターフェースカードからパケットデータ到着通知を受け取った場合のシーケンスを示す図である。

[0020] パケットデータの到着を検知したＮＩＣから、パケットデータ到着通知が割り込みの信号などによって通知される（Ｓ４００）。

[0021] 次に、ＮＩＣドライバ４０７が、ネットワークインターフェースカードからデータを取得する。そして、リアルタイムＵＤＰ／ＩＰ４０６に、パケットデータを送付する（Ｓ４０１）。

[0022] リアルタイムＵＤＰ／ＩＰ４０６は、パケットデータのポート領域に格納された番号が、リアルタイムＯＳ側のソフトウェアで使用するポートの番号であるか否か判定する。前述の番号が、リアルタイムＯＳ側のソフトウェアで使用するポートの番号である場合には、Ｓ４０３に遷移する。前述の番号が、リアルタイムＯＳ側のソフトウェアで使用する番号でない場合には、Ｓ４０４に遷移する（Ｓ４０２）。

[0023] Ｓ４０３では、リアルタイムＵＤＰ／ＩＰ４０６は、パケットデータをリアルタイムＯＳ側の適切なソフトウェアに送付し、Ｓ４０５に遷移する（Ｓ４０３）。

[0024] ステップＳ４０４では、リアルタイムＵＤＰ／ＩＰ４０６は、パケットデータを、リアルタイムＮＩＣプロキシ４０５を経由して、汎用ＯＳ　ＮＩＣプロキシ４０３に送付する。汎用ＯＳ　ＮＩＣプロキシ４０３は、ネットワーク対応アプリ４０２にパケットデータを送付する（Ｓ４０４）。

[0025] そして、処理を終了する（Ｓ４０５）。

特許文献1：特開２００３―１８６５６１号公報（第８頁、図１等）

特許文献2：特表２００７―５００３８１号公報（第１７頁、図１等）

発明の開示

発明が解決しようとする課題

[0026] しかし、上記説明した従来技術では、以下のような問題が生じている。

[0027] 即ち、特許文献１の手法は、プログラムに対してハッシュ演算を行って、正当なプログラムであるか否かを判定する。

[0028] しかしながら、この手法では、不正なプログラムと正当なプログラムを差し替えることで、不正なプログラムが動作する場合でも、正当なプログラムであると判定されるという課題がある。

[0029] 図１９を用いて、前述の課題を簡単に説明する。

[0030] まず、Ｓ４１１で、不正なプログラムが処理を行う。そして、Ｓ４１１からＳ４１２に遷移する前に、不正なプログラムと正当なプログラムを差し替える。そして、Ｓ４１２に遷移する。

[0031] Ｓ４１２では、差し替えられた正当なプログラムに対してハッシュ値（認証子）を生成する。そのため、正しいプログラムによる処理が行われたと判断されてしまう。

[0032] また、特許文献２の手法は、デバイスが扱うデータを、リアルタイムＯＳ側のソフトウェアか、または汎用ＯＳ側のソフトウェアかの、いずれで処理を行うかを判定するのみであり、アプリが正当なものであるかの確認は行っていない。

[0033] そのため、ネットワーク対応アプリ４０２がＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｋｅｃｔ Ｌａｙｅｒ）等の安全な通信方式を用いなければならない場合であっても、不正なソフトが、汎用ＯＳ４０１上で動作して、ＳＳＬなしで通信を行うことが可能であるという課題がある。

[0034] 本発明は、前述の課題を解決するものであり、所定のアプリケーションの正当性を判断した後に前記所定のアプリケーションが別の不正なアプリケー

ションに書換え、前記不正なアプリケーションによりデバイスが制御されるのを防止できる情報処理装置及びその制御方法を提供することを目的とする。

課題を解決するための手段

[0035] 前記従来の課題を解決するために、本発明に係る情報処理装置は、所定のデバイスにアクセスする所定のアプリケーションが動作するワークエリア上に前記所定のアプリケーションを書換え可能なものとして管理する仮想マシンと、前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、前記所定のアプリケーションの正当性を検証する検証部と、前記仮想マシン、前記検証部及び前記検出部を管理する仮想マシンモニタと、を具備し、前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直してその旨を前記検証部に通知し、前記検証部は前記仮想マシンモニタからの通知を受けると前記所定のアプリケーションが正当であるか否かを判断するものである。

発明の効果

[0036] このような構成により、本発明の情報処理装置は、前記仮想マシンモニタが前記ワークエリアに前記所定のアプリケーションを書換え不可能なものと管理し直した後に前記検証部が前記所定のアプリケーションが正当であるか否かを判断することにより、前記検証部が前記所定のアプリケーションの正当性を検証する前に前記所定のアプリケーションを書換え不可能に管理するので、前記検証部が前記所定のアプリケーションが正当なものと判断した後に前記所定のアプリケーションがワークエリア上で別の不正なアプリケーションに書き換えられるのを防止できる。

[0037] 本発明の請求項１に記載の情報処理装置は、所定のデバイスにアクセスする所定のアプリケーションをワークエリア上で動作させる仮想マシンと、前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記

仮想マシンから検出する検出部と、前記所定のアプリケーションの正当性を検証する検証部と、前記仮想マシン、前記検証部及び前記検出部を管理し、前記ワークエリア上で動作する所定のアプリケーションを書き換え可能に管理する仮想マシンモニタと、を具備し、前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直してその旨を前記検証部に通知し、前記検証部は前記仮想マシンモニタからの通知を受けると前記所定のアプリケーションが正当であるか否かを判断するものである。

[0038] 本発明によると、前記仮想マシンモニタが前記ワークエリアに前記所定のアプリケーションを書換え不可能なものと管理し直した後に前記検証部が前記所定のアプリケーションが正当であるか否かを判断することにより、前記検証部が前記所定のアプリケーションの正当性を検証する前に前記所定のアプリケーションを書換え不可能に管理するので、前記検証部が前記所定のアプリケーションが正当なものと判断した後に前記所定のアプリケーションがワークエリア上で別のアプリケーションに書き換えられるのを防止できる。

[0039] また、本発明の請求項２記載の情報処理装置は、請求項１記載の情報処理装置において、前記検証部が前記所定のアプリケーションが正当であると判断した場合、前記所定のアプリケーションを用いて所定のデバイスにアクセスする実行部を設けたものである。

[0040] 本発明によると、前記仮想マシンモニタが前記ワークエリアに前記所定のアプリケーションを書換え不可能なものと管理し直した後に、前記所定のアプリケーションが正当であるか否かを判断し、前記所定のアプリケーションを用いた所定のデバイスへのアクセスを実行することにより、前記検証部が前記所定のアプリケーションの正当性を検証する前に前記所定のアプリケーションを書換え不可能に管理するので、前記検証部が前記所定のアプリケーションが正当なものと判断した後に前記所定のアプリケーションがワークエリア上で別の不正なアプリケーションに書き換えられて、この不正なアプリ

ケーションを用いて所定のデバイスがアクセスされるのを防止できる。

[0041] また、本発明の請求項３記載の情報処理装置は、請求項２記載の情報処理装置において、前記仮想マシンモニタは、前記実行部が前記所定のアプリケーションを用いた所定のデバイスへのアクセスを終了した後、前記所定のアプリケーションを書換え可能なものに管理を戻すものである。

[0042] 本発明によると、前記仮想マシンモニタに、前記実行部が前記所定のアプリケーションを用いた所定のデバイスへのアクセスを終了した後、前記所定のアプリケーションを書換え可能なものに管理を戻させることにより、前記所定のアプリケーションによるアクセスが終了した後は前記所定のアプリケーションをワークエリアから消去できるので、処理後のアプリケーションによりワークエリアが無駄に占有されるのを防止できる。

[0043] また、本発明の請求項４記載の情報処理装置は、請求項１記載の情報処理装置において、前記仮想マシンモニタは、前記ワークエリアに前記所定のアプリケーションに対応する管理情報を管理し、前記管理情報は前記管理情報を書換える権限を有する主体を示す特権情報を含み、前記所定のアプリケーションの書換え可能な主体が前記仮想マシンを含む旨を前記特権情報が示している場合、前記所定のアプリケーションの書換え可能な主体から前記仮想マシンを排除するように前記特権情報を書き換えることで、前記所定のアプリケーションを書換え不可能なものと管理するものである。

[0044] 本発明によると、前記仮想マシンにより書換え可能な管理情報を、前記仮想マシンモニタが前記管理情報の中の特権情報を書換えることにより、前記仮想マシンによる前記所定のアプリケーションの書換えを不可能なものとするので、一旦前記仮想マシンモニタが前記特権情報を書換えると、前記仮想マシンモニタの方で前記仮想マシンによる前記管理情報の書換えを禁止できる。その結果、前記検証部が前記所定のアプリケーションが正当なものか否かを判断した後に前記所定のアプリケーションがワークエリア上で別のアプリケーションに書き換えられるのを確実に防止できる。

[0045] また、前記仮想マシンモニタは、前記管理情報の中の一部の情報である特

権情報を書き換えることにより、前記所定のアプリケーションの書換え可能な主体から前記仮想マシンを排除するので、簡易に前記仮想マシンモニタの方で前記仮想マシンによるワークエリア上で動作するアプリケーションの書換えを禁止できる。　さらに、前記管理情報の中の特権情報という既存の情報を書き換えることにより、前記仮想マシンによる前記管理情報の書換えを禁止するための別のデータ構造を不要とするので、書換え禁止にするための構成をシンプルにできる。

[0046] また、本発明の請求項５記載の情報処理装置は、請求項４記載の情報処理装置において、前記仮想マシンモニタは、前記所定のアプリケーションの書換え可能な主体を前記仮想マシン及び前記仮想マシンモニタを含む情報から、前記所定のアプリケーションの書換え可能な主体を前記仮想マシンモニタに制限する情報に前記特権情報を書き換えることで、前記所定のアプリケーションの書換え可能な主体から前記仮想マシンを排除するものである。

[0047] 本発明によると、前記所定のアプリケーションの書換え可能な主体を前記仮想マシン及び前記仮想マシンモニタを含む情報から、前記所定のアプリケーションの書換え可能な主体を前記仮想マシンモニタに制限する情報に前記特権情報を書き換えることにより、前記所定のアプリケーションの書換え可能な主体から前記仮想マシンを排除するので、簡易に前記仮想マシンによるワークエリア上で動作するアプリケーションの書換えを禁止できる。

[0048] また、本発明の請求項６記載の情報処理装置は、請求項１記載の情報処理装置において、前記所定のデバイスは、ＳＤカードとしたものである。

[0049] また、本発明の請求項７記載の情報処理装置は、請求項１記載の情報処理装置において、前記所定のデバイスは、前記情報処理装置にコンテンツを提供する外部のコンテンツサーバとしたものである。

[0050] また、本発明の請求項８記載の情報処理装置は、所定のデバイスにアクセスする前記所定のアプリケーションをワークエリア上で動作させる仮想マシンと、前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、前記仮想マシン及び前記検出部

を管理し、前記ワークエリア上で動作する所定のアプリケーションを書き換え可能に管理する仮想マシンモニタと、を具備し、前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直して、その旨を検証部を備える外部装置に通知し、前記外部装置の検証部に前記所定のアプリケーションが正当であるか否かの判断を行わせることを特徴としたものである。

[0051] 本発明によると、前記検証部は、前記情報処理装置の内部ではなく、前記情報処理装置の外部装置に含まれるものであってもよい。

[0052] また、本発明の請求項９記載の情報処理装置は、所定のデバイスにアクセスする所定のアプリケーションをワークエリア上で動作させる仮想マシンと、前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、前記仮想マシン及び前記検出部を管理し、前記ワークエリア上で動作する所定のアプリケーションを書き換え可能に管理する仮想マシンモニタと、サービスを提供する実行部を備える外部装置と通信する通信部と、を具備し、前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直し、前記通信部は、前記所定のアプリケーションが書換え不可能なものと管理し直された後に正当なものであると判断された場合に、前記外部装置の実行部から前記サービスの提供を受けることを特徴としたものである。

[0053] 本発明によると、前記実行部は、前記情報処理装置の内部ではなく、前記情報処理装置の外部装置に含まれるものであってもよい。

[0054] また、本発明の請求項１０に記載の情報処理装置の制御方法は、所定のデバイスにアクセスする所定のアプリケーションをワークエリア上で動作させる仮想マシンと、前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、前記所定のアプリケーションの正当性を検証する検証部と、前記仮想マシン、前記検証部及び前

記検出部を管理する仮想マシンモニタと、を具備した情報処理装置において、前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直してその旨を前記検証部に通知し、前記検証部は前記仮想マシンモニタからの通知を受けると前記所定のアプリケーションが正当であるか否かを判断するようにしたものである。

[0055] 本発明によると、前記仮想マシンモニタが前記ワークエリアに前記所定のアプリケーションを書換え不可能なものと管理し直した後に前記検証部が前記所定のアプリケーションが正当であるか否かを判断することにより、前記検証部が前記所定のアプリケーションの正当性を検証する前に前記所定のアプリケーションを書換え不可能に管理するので、前記検証部が前記所定のアプリケーションが正当なものと判断した後に前記所定のアプリケーションがワークエリア上で別の不正なアプリケーションに書き換えられるのを防止できる。

[0056] また、本発明の請求項１１に記載の情報処理装置の制御プログラムは、所定のデバイスにアクセスする所定のアプリケーションをワークエリア上で動作させる仮想マシンと、前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、前記所定のアプリケーションの正当性を検証する検証部と、前記仮想マシン、前記検証部及び前記検出部を管理する仮想マシンモニタと、を具備した情報処理装置の制御プログラムであって、前記検出部が前記アクセス要求を検出すると、その旨を前記仮想マシンモニタに通知するステップと、前記仮想マシンモニタに、前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直させ、その旨を前記検証部に通知させるステップと、前記仮想マシンモニタからの通知を受けた前記検証部に、前記所定のアプリケーションが正当であるか否かを判断させるようにしたものである。

[0057] 本発明によると、前記仮想マシンモニタが前記ワークエリアに前記所定のアプリケーションを書換え不可能なものと管理し直した後に前記検証部が前

記所定のアプリケーションが正当であるか否かを判断することにより、前記検証部が前記所定のアプリケーションの正当性を検証する前に前記所定のアプリケーションを書換え不可能に管理するので、前記検証部が前記所定のアプリケーションが正当なものと判断した後に前記所定のアプリケーションがワークエリア上で別の不正なアプリケーションに書き換えられるのを防止できる。

[0058] また、本発明の請求項１２に記載の情報処理装置の集積回路は、所定のデバイスにアクセスする所定のアプリケーションをワークエリア上で動作させる仮想マシンと、前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、前記所定のアプリケーションの正当性を検証する検証部と、前記仮想マシン、前記検証部及び前記検出部を管理する仮想マシンモニタと、を具備し、前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直してその旨を前記検証部に通知し、前記検証部は前記仮想マシンモニタからの通知を受けると前記所定のアプリケーションが正当であるか否かを判断するようにしたものである。

[0059] 本発明によると、前記仮想マシンモニタが前記ワークエリアに前記所定のアプリケーションを書換え不可能なものと管理し直した後に前記検証部が前記所定のアプリケーションが正当であるか否かを判断することにより、前記検証部が前記所定のアプリケーションの正当性を検証する前に前記所定のアプリケーションを書換え不可能に管理するので、前記検証部が前記所定のアプリケーションが正当なものと判断した後に前記所定のアプリケーションがワークエリア上で別の不正なアプリケーションに書き換えられるのを防止できる。

図面の簡単な説明

[0060] [図1]本発明の実施の形態１のソフトウェア構成を示すブロック図である。

[図2]本発明の実施の形態１のハードウェア構成を示すブロック図である。

[図3]本発明の実施の形態１の情報処理装置の物理メモリ空間を示す図である。

[図4]本発明の実施の形態１の仮想物理メモリ空間と論理メモリ空間との対応関係の一例を示す図である。

[図5]本発明の実施の形態１のページテーブルのデータ構造の一例を示す図である。

[図6]本発明の実施の形態１のＣＰＵが、通常メモリ及び保護メモリへアクセスを行った場合のアクセス制御を示す図である。

[図7]本発明の実施の形態１の汎用ＯＳによるページテーブルとアプリケーションの操作の一例を示す図である。

[図8]本発明の実施の形態１のセキュアＶＭＭによるページテーブルとソフト実行環境の操作の一例を示す図である。

[図9]本発明の実施の形態１の不正アプリケーションによる、セキュアデバイスアクセス防止を示すシーケンス図である。

[図10]本発明の実施の形態２のソフトウェア構成を示す図である。

[図11]本発明の実施の形態２の情報処理装置とアプリ判定サーバとがネットワーク接続された構成を示す図である。

[図12]本発明の実施の形態３のソフトウェア構成を示す図である。

[図13]本発明の実施の形態３の情報処理装置とアプリ判定サーバとサービス提供サーバとがネットワーク接続された構成を示す図である。

[図14]本発明の実施の形態３の不正アプリケーションによる、セキュアデバイスアクセス防止を示すシーケンス図である。

[図15]本発明の実施の形態４のソフトウェア構成を示す図である。

[図16]本発明の実施の形態４の不正アプリケーションによる、セキュアデバイスアクセス防止を示すシーケンス図である。

[図17]本発明の実施の形態５のソフトウェア構成を示す図である。

[図18]本発明の実施の形態５の不正アプリケーションによる、セキュアデバイスアクセス防止を示すシーケンス図である。

[図19]従来のプログラムの正当性を確認するシーケンス図

[図20]従来のＯＳ仮想化実行環境における、データを適切に実行環境ごとに処理するソフトウェア構成を示す図である。

[図21]従来のＯＳ仮想化実行環境における、データを適切に実行環境ごとに処理するシーケンス図である。

[図22]汎用ＯＳ上のアプリケーションをロードするシーケンス図である。

[図23]本発明の実施の形態１のページテーブルのデータ構造の書換え後一例を示す図である。

符号の説明

[0061] １００、１３３、１９０、２００、２３０、２６０、２８０　セキュアＶＭＭ

１０１、１２９、１８０、２０１、２３１、２６１、２８１、４０１　汎用ＯＳ

１０２、１０３、１２７、１２８、１８３、１８４、２０２、２０３、２３２、２３３、２６２、２６３、２８２、２８３　アプリケーション

１０４、１３２、２０４、２３４、２６４、２８４　管理専用ＯＳ

１０５、１３０、２０５、２６５、２８５　セキュアデバイスドライバ

１０６、１３１、２０６、２３６、２６６、２８６　アプリ特定部

１０７、２０７、２３７、２６７、２８７　動作アプリ格納メモリ特定部

１０８、２０８、２３８、２６８、２８８　動作アプリメモリロック部

１０９、２０９、２３９、２６９、２９０　デバイスアクセス要求判定部

１１０、２１０、２７０、２９１　デバイスアクセス制御部

１１１、２１１、２４０、２７１、２８９　認証子生成部

１１２、２２３、２５４、２７２、２９２　アプリ判定部

１２０、２２０、２５０　情報処理装置

１２１　ＣＰＵ

１２２　ＭＭＵ

１２３、１４１、１５１　通常メモリ

１２４、１４３　保護メモリ

１２５　バス

１２６　セキュアデバイス

１３４　不揮発性記憶装置

１４０　情報処理装置の物理メモリ空間

１４２、１４４、１５２　予約領域

１５０　セキュアＶＭＭによって、汎用ＯＳに割り当てられた仮想物理メモリ空間

１３５、１３６、１５３、１６０、１８１、１８２、３００　ページテーブル

１５４　アプリケーションの論理メモリ空間

１６１、３０１　ページ番号のフィールド

１６２、３０２　論理アドレス番号のフィールド

１６３、３０３　仮想物理アドレス番号のフィールド

１６４、３０４　特権情報のフィールド

１６５、３０５　書込み操作許可・不許可情報のフィールド

１６６、３０６　読込み操作許可・不許可情報のフィールド

１６７、３０７　その他の情報のフィールド

１７０　通常メモリ及び保護メモリへアクセスを行った場合のアクセス制御を示すテーブル

１９１　汎用ＯＳが管理するカレントページテーブル

１９２　管理専用ＯＳが管理するカレントページテーブル

１９３　汎用ＯＳと動作中のアプリケーション

１９４　管理専用ＯＳと動作中の管理専用ＯＳ上のアプリケーション

２１２、２４１　通信部

２２１、２５１　アプリ判定サーバ

２２２、２５３　ネットワーク

２３５　ネットワークインターフェースドライバ

２５２　サービス提供サーバ

２５５　サービス提供部

２５６　サービス提供判定部

４００　ＶＭＭ

４０２　ネットワーク対応アプリ

４０３　汎用ＯＳ　ＮＩＣプロキシ

４０４　リアルタイムＯＳ

４０５　リアルタイムＮＩＣプロキシ

４０６　リアルタイムＵＤＰ／ＩＰ

４０７　ＮＩＣドライバ

発明を実施するための最良の形態

[0062] 以下に、本発明の実施の形態について、図面を参照しながら説明を行う。

[0063] （実施の形態１）

＜実施の形態１のソフトウェアの構成の説明＞

図１は、本発明の実施の形態１に関わるソフトウェア構成を示す図である。

[0064] 実施の形態１の情報処理装置は、仮想マシンモニタであるセキュアＶＭＭ１００と、汎用ＯＳ１０１と、アプリケーションＡ　１０２と、アプリケーションＢ　１０３と、管理専用ＯＳ１０４と、検出部であるデバイスアクセス要求判定部１０９及び実行部であるセキュアアクセス制御部１１０を含むセキュアデバイスドライバ１０５と、検証部であるアプリ特定部１０６と、から構成される。仮想マシンは、汎用ＯＳ１０１と、アプリケーションＡ１０２と、アプリケーションＢ１０３を含む。

[0065] セキュアＶＭＭ１００は、ＯＳ仮想化機能を提供する。汎用ＯＳ１０１と管理専用ＯＳ１０４は、セキュアＶＭＭ１００が提供する仮想化されたハードウェア上で動作するオペレーティングシステムである。

[0066] セキュアＶＭＭ１００は、動作アプリ格納メモリ特定部１０７と、動作アプリメモリロック部１０８とを備える。

[0067] アプリケーションＡ　１０２とアプリケーションＢ　１０３は、ユーザに対してサービスを提供するアプリケーションであり、必要に応じて、図示していないセキュアデバイスにアクセスする。

[0068] セキュアデバイスドライバ１０５は、図示してないセキュアデバイスを制御するデバイスドライバであり、デバイスアクセス要求判定部１０９と、デバイスアクセス制御部１１０を備える。

[0069] アプリ特定部１０６は、認証子生成部１１１と、アプリ判定部１１２を備える。

[0070] ＜セキュアＶＭＭの構成要素の説明＞

動作アプリ格納メモリ特定部１０７は、図示していないセキュアデバイスへのアクセスを行う汎用ＯＳ１０１上のアプリケーションを特定する。詳細は後述する。

[0071] 動作アプリメモリロック部１０８は、図示していないセキュアデバイスへのアクセスを行う汎用ＯＳ１０１上のアプリケーションに対応するページテーブルに対して、制御を行う。詳細は後述する。

[0072] ＜セキュアデバイスドライバの構成要素の説明＞

デバイスアクセス要求判定部１０９は、図示していないセキュアデバイスへのアクセス要求を検出する。詳細は後述する。

[0073] デバイスアクセス制御部１１０は、図示していないセキュアデバイスへのアクセス制御を行う。詳細は後述する。

[0074] ＜アプリ特定部の構成要素の説明＞

認証子生成部１１１は、図示していないセキュアデバイスに対して、汎用ＯＳ１０１上のアプリケーションの認証子を生成する。詳細は後述する。

[0075] アプリ判定部１１２は、前述のアプリケーションの認証子を用いて、アプリケーションが正当であるか否かを判定する。詳細は後述する。

[0076] ＜実施の形態１のハードウェアの構成の説明＞

図２は、図１のソフトウェアが動作する情報処理装置１２０のハードウェア構成図である。

[0077] 図２において、情報処理装置１２０は、ＣＰＵ１２１と、ＭＭＵ（Ｍｅｍｏｒｙ Ｍａｎａｇｅｍｅｎｔ Ｕｎｉｔ）１２２と、通常メモリ１２３と、保護メモリ１２４と、セキュアデバイス１２６と、不揮発性記憶装置１３４が、バス１２５を介して互いに接続している。

[0078] 情報処理装置１２０は、さらに、図２に図示されていない入出力部や補助記憶装置などを備えているが、これらは本発明の本質ではないので説明を省略する。

[0079] 以下、情報処理装置１２０の各構成要素の詳細について説明する。

[0080] ＜情報処理装置のハードウェアの構成要素の説明＞

ＣＰＵ１２１は、通常メモリ１２３や保護メモリ１２４に格納されたプログラム等に含まれる命令コードを実行することにより、情報処理装置１２０全体の動作を制御する。

[0081] ＭＭＵ１２２は、図示していないページテーブルを参照して、ＣＰＵ１２１に対して、物理アドレス番号を論理アドレス番号に変換する機能を提供する。さらに、ＭＭＵ１２２は、図示していないページテーブルを参照して、ＣＰＵ１２１の特権状態に応じて、メモリへの書込み操作や読み込み操作などのアクセス制御機能を提供する。

[0082] 不揮発性記憶装置１３４は、アプリケーションＡ　１２７と、アプリケーションＢ　１２８とを格納する不揮発性の記憶装置である。具体的には、ハードディスクやフラッシュメモリなどである。

[0083] 通常メモリ１２３は、不揮発性記憶装置１３４に格納されているアプリケーションＡ　１２７と、アプリケーションＢ　１２８と、汎用ＯＳ１２９とをロードして、実行される揮発性記憶装置である。本発明のワークエリアに当たる。

[0084] 保護メモリ１２４は、セキュアデバイスドライバ１３０と、アプリ特定部１３１と、管理専用ＯＳ１３２と、セキュアＶＭＭ１３３とを格納する記憶装置である。

[0085] セキュアデバイス１２６は、コンテンツなどの保護すべき情報を取り扱う

デバイスであり、不正なアプリケーションからのアクセスを防止する必要があるデバイスである。例えば、暗号化コンテンツの復号などを行う暗復号回路などである。他の例として、暗号化したコンテンツを記録したフラッシュメモリ等の記録媒体や、復号化されたコンテンツが保持されるメモリなどが考えられる。また、セキュアデバイスは情報処理装置に内蔵されたものに限らず、ＳＤカード等の外部の記録装置であってもよい。

[0086] さらに、保護メモリ１２４とセキュアデバイス１２６は、保護メモリ１２４に格納されたソフトウェアのみがアクセス可能となるように制御される。

[0087] ＜汎用ＯＳとアプリケーションとの関連性の説明＞

汎用ＯＳ１２９は、汎用ＯＳ１２９上で動作するアプリケーションＡ　１２７とアプリケーションＢ　１２８に対応して、それぞれページテーブル１３５とページテーブル１３６を保持する。なお、ページテーブルに関する詳細は後述する。

[0088] ＜ＯＳ仮想化機能を用いた場合のメモリ空間の説明＞

図３は、情報処理装置１２０の物理メモリ空間１４０を示す図である。

[0089] 情報処理装置１２０の物理メモリ空間１４０は、通常メモリに対応するメモリ空間１４１と、予約領域Ａ　１４２と、保護メモリに対応するメモリ空間１４３と、予約領域Ｂ　１４４とで構成される。情報処理装置の物理メモリ空間１４０は、物理メモリ番地で一意に特定する事が可能である。

[0090] セキュアＶＭＭ１００は、情報処理装置の物理メモリ空間１４０を、汎用ＯＳ１０１に割り当てられた物理メモリ空間と、管理専用ＯＳ１０４に割り当てられた物理メモリ空間に分割して管理する。

[0091] 汎用ＯＳ１０１に割り当てられた物理メモリ空間は、通常メモリに対応するメモリ空間１４１と、予約領域Ａ　１４２とで構成される。

[0092] 管理専用ＯＳ１０４に割り当てられた物理メモリ空間は、保護メモリに対応するメモリ空間１４３と、予約領域Ｂ　１４４とで構成される。

[0093] セキュアＶＭＭ１００は、汎用ＯＳ１０１と管理専用ＯＳ１０４に対して、それぞれのメモリ空間を、仮想物理アドレス空間として参照させる。汎用

ＯＳ１０１と管理専用ＯＳ１０４は、それぞれの仮想物理アドレス空間に対して、仮想物理アドレス番号を用いて、読み込み操作及び書込み操作を行う。

[0094] ＜仮想物理メモリ空間と論理メモリ空間の説明＞

図４は、仮想物理メモリ空間と論理メモリ空間との対応関係を示す一例の図である。なお、図４の仮想物理メモリ空間は、汎用ＯＳが読み込み操作及び書込み操作を行う仮想物理メモリ空間である。

[0095] 通常メモリ１５１は、ページと呼ばれる固定長サイズに分割されて管理される。

[0096] ページテーブル１５３は、複数のページをまとめて管理し、論理アドレス空間を構築する。さらに、１つのページテーブルが、１つのアプリケーションに対応する。

[0097] アプリケーションは、論理アドレス空間に対して、論理アドレス番号を用いて読み込み操作及び書込み操作を行う。

[0098] ＜ページテーブルの構成要素の説明＞

図５は、ページテーブル１６０のデータ構造の一例を示す図である。

[0099] ページテーブル１６０は、ページに対応する各エントリに対して、ページ番号１６１と、論理アドレス番号１６２と、仮想物理アドレス番号１６３と、特権情報１６４と、書込み操作許可・不許可情報１６５と、読込み操作許可・不許可情報１６６と、その他の情報１６７と、から構成されるデータ構造である。

[0100] ページ番号１６１は、ページの番号を格納するフィールドである。

[0101] 論理アドレス番号１６２は、ＭＭＵ１２２が仮想物理アドレス番号を論理アドレス番号に変換する際の対応する論理アドレス番号を格納するフィールドである。本フィールドは、各仮想物理アドレス番号に対応する論理アドレス番号それぞれを格納していてもよいし、ページの先頭論理アドレス番号が格納していてもよい。

[0102] 仮想物理アドレス番号１６３は、ＭＭＵ１２２が仮想物理アドレス番号を

論理アドレス番号に変換する際の対応する仮想物理アドレス番号を格納するフィールドである。本フィールドは、ページの先頭仮想物理アドレス番号が格納されていてもよい。

[0103] 特権情報１６４は、ＭＭＵ１２２がメモリへのアクセス制御を行う場合に参照する特権情報に関する情報を格納するフィールドである。詳細は後述する。

[0104] 書込み操作許可・不許可情報１６５は、ページテーブル１６０に対応するアプリケーションが、ページへの書込み操作を行ってもよいか否かを示すフィールドである。本フィールドには、許可または不許可を示す情報が格納される。

[0105] 読込み操作許可・不許可情報１６６は、ページテーブル１６０に対応するアプリケーションが、ページへの読込み操作を行ってもよいか否かを示すフィールドである。本フィールドには、許可または不許可を示す情報が格納される。

[0106] その他の情報１６７は、ページのサイズや、ページのダーティ情報や、前述の属性以外の情報などが格納されているフィールドである。

[0107] また、ページテーブルの各フィールドの情報の変更は、ＣＰＵ１２１の特権状態がリング０の場合のみ可能である。なお、特権状態に関しては、詳細は後述する。

[0108] なお、図５で示したページテーブル１６０は論理的なデータ構造であり、例えば、公知の階層的なページテーブル構造を用いてもよい。

[0109] なお、図５で示したページテーブル１６０では、各ページ毎に特権情報が割り当てられているが、１つのページテーブルに対して１つの特権情報を割り当てても良い。その場合には、前記の１つの特権情報は、別のデータ構造やレジスタで管理しても良い。

[0110] 図５で示したページテーブル１６０では、書込み操作許可・不許可情報１６５は、アプリケーションからの書込みが可能か否かを示すフィールドであるが、それ以外であってもよい。例えば、その他の情報１６７に格納されて

いる書込み操作主体を示す情報と組み合わせて、前記主体が書込み操作が可能か否かを示すフィールドであってもよい。

[0111] 図５で示したページテーブル１６０では、読込み操作許可・不許可情報１６６は、アプリケーションからの読込みが可能か否かを示すフィールドであるが、それ以外であってもよい。例えば、その他の情報１６７に格納されている読込み操作主体を示す情報と組み合わせて、前記主体が読込み操作が可能か否かを示すフィールドであってもよい。

[0112] ＜ＣＰＵの特権状態によるメモリアクセス制御の説明＞

図６は、ＣＰＵ１２１が、通常メモリ１２３及び保護メモリ１２４へアクセスを行った場合のアクセス制御を示す表である。

[0113] 図６のアクセス制御は、ＣＰＵ１２１で実現しても良いし、ＭＭＵ１２２で実現しても良い。

[0114] ＣＰＵ１２１には、リング０、リング１、リング２、リング３という特権状態がある。ＣＰＵ１２１は、特権命令を実行することで、各特権状態を遷移する。

[0115] 特権状態リング０であるＣＰＵ１２１で動作する主体であるソフトウェアは、ページテーブル１６０の特権情報１６４フィールドが、リング０とリング１とリング２とリング３のページにアクセスすることができる。また、特権情報１６４フィールドがリング０とリング１とリング２とリング３のページテーブルの内容を書き換えることができる。

[0116] 特権状態リング１であるＣＰＵ１２１で動作する主体であるソフトウェアは、ページテーブル１６０の特権情報１６４フィールドが、リング１とリング２とリング３のページにアクセスすることができる。また、特権情報１６４フィールドがリング１とリング２とリング３のページテーブルの内容を書き換えることができる。特権状態リング１であるＣＰＵ１２１で動作する主体であるソフトウェアが、ページテーブル１６０の特権情報１６４フィールドが、リング０のページにアクセスした場合には、ＣＰＵ１２１またはＭＭＵ１２２が、不正なメモリアクセスであることを検出し、アクセスを拒否す

る。

[0117] 特権状態リング２であるＣＰＵ１２１で動作する主体であるソフトウェアは、ページテーブル１６０の特権情報１６４フィールドが、リング２とリング３のページにアクセスすることができる。また、特権情報１６４フィールドがリング２とリング３のページテーブルの内容を書き換えることができる。特権情報リング２であるＣＰＵ１２１で動作する主体であるソフトウェアが、ページテーブル１６０の特権情報１６４フィールドが、リング０とリング１のページにアクセスした場合には、ＣＰＵ１２１またはＭＭＵ１２２が、不正なメモリアクセスであることを検出し、アクセスを拒否する。

[0118] 特権状態リング３であるＣＰＵ１２１で動作する主体であるソフトウェアは、ページテーブル１６０の特権情報１６４フィールドが、リング３のページにアクセスすることができる。また、特権情報１６４フィールドがリング３のページテーブルの内容を書き換えることができる。特権状態リング３であるＣＰＵ１２１で動作する主体であるソフトウェアが、ページテーブル１６０の特権情報１６４フィールドが、リング０とリング１とリング２のページにアクセスした場合には、ＣＰＵ１２１またはＭＭＵ１２２が、不正なメモリアクセスであることを検出し、アクセスを拒否する。

[0119] また、情報処理装置１２０において、リング０にはセキュアＶＭＭ１００が割り当てられ、リング１には管理専用ＯＳ１０４が割り当てられ、リング２には汎用ＯＳ１０１が割り当てられ、リング３には汎用ＯＳ上で動作するアプリケーションが割り当てられている。

[0120] なお、特権の割り当て方法は、前述のリングの割り当てには限らない。汎用ＯＳ１０１と汎用ＯＳ上で動作するアプリケーションが割り当てられた特権が、セキュアＶＭＭ１００と管理専用ＯＳ１０４が割り当てられた特権より低くなるように制御できれば他の割り当て方法を用いてもよい。

[0121] ＜アプリケーションのロード処理の説明＞

図２２は、汎用ＯＳによるアプリケーションのロード処理を示すシーケンス図である。

[0122] 図示されていないインターフェースによるユーザの指示などによって、アプリケーションのロード処理が開始される（Ｓ３００）。

[0123] 汎用ＯＳ１８０は、不揮発性記憶装置１３４から、アプリケーションが格納されているファイルを読み込む（Ｓ３０１）。

[0124] 汎用ＯＳ１８０は、ファイルのヘッダファイルに格納されている必要メモリサイズなどを参照して、アプリケーションに割り当てるメモリサイズを算出し、通常メモリ１２３から必要なメモリ領域を確保する（Ｓ３０２）。

[0125] 汎用ＯＳ１８０は、アプリケーションに対応するページテーブルを内部に作成する（Ｓ３０３）。

[0126] 汎用ＯＳ１８０は、ステップＳ３０２で確保したメモリ領域に、ステップＳ３０１で読み込んだファイルからアプリケーションのプログラム（コードとデータ）をロードする（Ｓ３０４）。

[0127] そして、汎用ＯＳ１８０は、アプリケーションのロード処理を終了する（Ｓ３０５）。

[0128] なお、ステップＳ３０４とステップＳ３０５は、逆の順序で実施されてもよい。

[0129] ＜ＯＳによるページテーブルとアプリケーションの操作の説明＞

図７は、汎用ＯＳによるページテーブルとアプリケーションの操作の一例を示す図である。図７において、汎用ＯＳ１８０上で、アプリケーションＡ　１８３とアプリケーションＢ　１８４が動作している。

[0130] 汎用ＯＳ１８０は、アプリケーションＡ　１８３とアプリケーションＢ　１８４に、ＣＰＵを、時分割で割り当てることで、アプリケーションＡ　１８３とアプリケーションＢ　１８４を動作させる。

[0131] 前述の時分割で割り当てる操作において、汎用ＯＳ１８０は、アプリケーションＡ　１８３とアプリケーションＢ　１８４を切り替える。その切り替え操作は、各アプリケーションに対応するページテーブルを切り替えることで実現する。

[0132] 図７の場合には、汎用ＯＳ１８０は、アプリケーションＡ　１８３に対応

するページテーブル１８１と、アプリケーションＢ　１８４に対応するページテーブル１８２と、を保持し、切り替えることで、アプリケーションを時分割で実行する。

[0133] また、管理専用ＯＳ１０４も、同様のページテーブルの操作を行うことで、管理専用ＯＳ１０４上で動作するソフトウェアを切り替える。

[0134] ＜セキュアＶＭＭによるページテーブルとソフト実行環境の操作の説明＞

図８は、セキュアＶＭＭによるページテーブルとソフト実行環境の操作の一例を示す図である。図８において、セキュアＶＭＭ１９０上で、汎用ＯＳ１９３と管理専用ＯＳ１９４が動作している。

[0135] セキュアＶＭＭ１９０は、汎用ＯＳ１９３と管理専用ＯＳ１９４に、ＣＰＵを、時分割で割り当てることで、汎用ＯＳ１９３と管理専用ＯＳ１９４を動作させる。

[0136] 前述の時分割で割り当てる操作において、セキュアＶＭＭ１９０は、汎用ＯＳ１９３と管理専用ＯＳ１９４を切り替える。その切り替え操作は、各ＯＳ（ソフト実行環境）に対応するカレントページテーブルを切り替えることで実現する。ここで、カレントページテーブルとは、各ＯＳが現在ＣＰＵ１２１に参照させているページテーブルである。

[0137] 図８の場合には、セキュアＶＭＭ１９０は、汎用ＯＳ１９３に対応するカレントページテーブル１９１と、管理専用ＯＳ１９４に対応するカレントページテーブル１９２と、を保持し、切り替えることで、各ＯＳ（ソフト実行環境）を時分割で実行する。

[0138] ＜不正アプリによるセキュアデバイスアクセスの検出及びアクセス防止の説明＞

以下に、図９を用いて、情報処理装置１２０が、不正アプリによるセキュアデバイスアクセスの検出及びアクセス防止の説明を行う。

[0139] 汎用ＯＳ１０１上のアプリケーションが、汎用ＯＳ１０１を介して、セキュアデバイス処理要求を行う（Ｓ１００）。

[0140] セキュアＶＭＭ１００は、前述のソフト実行環境の操作を用いて、汎用Ｏ

Ｓ１０１から管理専用ＯＳ１０４に切り替える。そして、処理要求検出ステップにおいて、セキュアデバイスドライバ１０５のデバイスアクセス要求判定部１０９が、前述のセキュアデバイス処理要求を検出する。そして、デバイスアクセス要求判定部１０９は、セキュアＶＭＭ１００に対して、対象アプリ抽出要求を行う（Ｓ１０１）。

[0141] 対象アプリ抽出要求に対して、セキュアＶＭＭ１００は、対象アプリ抽出ステップと対象アプリロックステップを行う。

[0142] 対象アプリ抽出ステップでは、セキュアＶＭＭ１００の動作アプリ格納メモリ特定部１０７が、汎用ＯＳ１０１のカレントページテーブルを抽出する。汎用ＯＳ１０１が動作させているアプリケーションはセキュアデバイス処理要求を出したアプリケーションであるので、カレントページテーブルはこのアプリケーションのページテーブルとなる（Ｓ１０２）。

[0143] 対象アプリロックステップでは、セキュアＶＭＭ１００の動作アプリメモリロック部１０８が、汎用ＯＳ１０１のカレントページテーブルに格納されている情報を、保護メモリにバックアップする。そして、動作アプリメモリロック部１０８が、汎用ＯＳ１０１のカレントページテーブルの書込み許可・不許可情報のフィールドを全て、「不許可」に変更する。例えば、図５に示すページテーブル１６０に前述の操作を行った場合には、図２３のページテーブル３００に変更される。書換え後のページテーブル３００では、書換え前のページテーブル１６０の特権情報１６４のフィールドのリング３が、ページテーブル３００の特権情報３０４で示すようにリング０に書き換えられる。さらに、書換え後のページテーブル３００では、書換え前のページテーブル１６０の書込み操作許可・不許可情報１６５のフィールドが、ページテーブル３００の書込み許可・不許可情報３０５で示すように全て「不許可」に書き換えられる。

[0144] これにより、セキュアデバイス処理要求を出したアプリケーションがロードされているメモリ空間の書き換えが不可能となる。さらに、特権情報のフィールドを、汎用ＯＳおよび汎用ＯＳ上で動作するアプリケーションに割り

当てられた特権では変更できないリング番号に変更する。この特権情報の変更により、汎用ＯＳおよび汎用ＯＳ上で動作するアプリケーションは、カレントページテーブルの元々の特権情報に関わらず、書込み許可・不許可情報のフィールドを「不許可」から「許可」に戻すことができなくなる。したがって、汎用ＯＳ側およびその上で動作するプリケーションによってページテーブルの書込み許可・不許可情報のフィールドを「許可」に戻し、アプリケーションがロードされているメモリ空間の書き換えを可能とするような攻撃も防げる。本実施の形態では、この書込み許可・不許可情報１６５のフィールドの書き換えと、特権情報のフィールドの書き換えにより、セキュアデバイス処理要求を出したアプリケーションを書換えることができる主体から汎用ＯＳおよび汎用ＯＳ上で動作する全アプリケーションを含めた仮想マシンを排除する。そして、アプリ特定部１０６に対して、アプリ特定要求を行う（Ｓ１０３）。

[0145] アプリ特定要求に対して、アプリ特定部１０６は、認証子生成ステップとアプリ判定ステップを行う。

[0146] 認証子生成ステップでは、アプリ特定部１０６の認証子生成部１１１が、前述の抽出されたページテーブルを用いて、論理アドレス空間を参照する。認証子生成部１１１が、参照した論理アドレス空間に格納されたプログラムから、ＳＨＡ１などの一方向性関数を用いて、ハッシュ値を生成する（Ｓ１０４）。

[0147] 次に、アプリ判定ステップでは、アプリ特定部１０６のアプリ判定部１１２が、予め保持している参照ハッシュ値と、前述の生成したハッシュ値とが一致するか否かを確認する。一致する場合には、アプリ判定部１１２が、Ｓ１００のセキュアデバイス処理要求を行ったアプリケーションは正当なアプリケーションであると判定する。一致しない場合には、アプリ判定部１１２が、Ｓ１００のセキュアデバイス処理要求を行ったアプリケーションは不正なアプリケーションであると判定する。アプリ判定部１１２が、前述の判定結果を用いて、セキュアデバイスドライバ１０５に対して、デバイスアクセ

ス制御要求を行う（Ｓ１０５）。

[0148] デバイスアクセス制御要求に対して、セキュアデバイスドライバ１０５のデバイスアクセス制御部１１０は、前述の判定結果が、正当なアプリケーションの場合には、セキュアデバイスへのアクセスを許可する。または、デバイスアクセス制御部１１０は、前述の判定結果が、不正なアプリケーションの場合には、セキュアデバイスへのアクセスを拒否する（Ｓ１０６）。

[0149] デバイスアクセス制御部１１０が、セキュアデバイスへのアクセスを許可した場合に、セキュアデバイスドライバ１０５は、セキュアデバイスに対する処理を行う（Ｓ１０７）。そして、処理終了後に、セキュアデバイスドライバ１０５は、セキュアＶＭＭ１００に対して、対象アプリロック解除要求を行う。

[0150] 対象アプリロック解除要求に対して、セキュアＶＭＭ１００の動作アプリメモリロック部１０８は、対象アプリロック解除ステップを行う。

[0151] 対象アプリロック解除ステップにおいて、動作アプリメモリロック部１０８は、バックアップしていたカレントページテーブルの情報を、汎用ＯＳ１０１のカレントページテーブルに再設定を行う。これにより、ページテーブルの書込み許可・不許可情報および特権情報が、対象アプリロックステップ以前の状態に戻る（Ｓ１０８）。

[0152] そして、セキュアＶＭＭ１００は、汎用ＯＳ１０１に切り替える。汎用ＯＳ１０１は、セキュアデバイスドライバ１０５の処理結果をアプリケーションに通知する。

[0153] また、ステップＳ１０６において、セキュアデバイスへのアクセスを拒否すると判断された場合には、セキュアデバイスドライバ１０５は、セキュアＶＭＭ１００に対して、対象アプリロック解除要求を行い、セキュアＶＭＭ１００の動作アプリメモリロック部１０８は、前述のステップＳ１０８と同様の処理を行う。そして、セキュアＶＭＭ１００は、汎用ＯＳ１０１に切り替える。汎用ＯＳは、セキュアデバイスドライバ１０５の処理結果をアプリケーションに通知する。

[0154] ＜実施の形態１の効果＞

上述した実施の形態１では、セキュアデバイス処理要求が検出されると、その要求を出したアプリケーションがロードされているページテーブルの設定を書き込み不可能とした上で、アプリケーションの検証を行っている。また、この書き込み不可能の設定は、セキュアデバイスへのアクセスが終了するまで解除されない。これにより、正当なアプリケーションで検証を通した上で、メモリ上のアプリケーションを不正なアプリケーションに上書きしてセキュアデバイスへの不正なアクセスを試みる攻撃を防止することが出来る。すなわち、アプリケーションがロードされているメモリを改変できないよう設定にした上でそのアプリケーションを検証しているので、検証が終了した直後にメモリ上のアプリケーションを不正なアプリケーションに差し替えることはできない。

[0155] さらに、ページテーブルの特権情報のフィールドを、汎用ＯＳおよび汎用ＯＳ上で動作するアプリケーションでは変更できない特権に書き換えることにより、汎用ＯＳ等からはページテーブルの設定を書込み許可に戻すことができなくなるようにしている。これにより、汎用ＯＳ上の不正なアプリケーションによってページテーブルの設定を書き込み許可に戻した上で、アプリケーションを差し替えるような攻撃をも防止することができる。

[0156] （実施の形態２）

図１０は、本発明の実施の形態２に関わる情報処理装置のソフトウェア構成を示すブロック図である。

[0157] 図１１は、本発明の実施の形態２に関わる情報処理装置とアプリ判定部とがネットワーク接続された構成を示す図である。

[0158] 実施の形態１の情報処理装置１２０と実施の形態２の情報処理装置２２０との構成の差異は以下の通りである。

[0159] 実施の形態１の情報処理装置１２０では、アプリ特定部１０６が、検証部であるアプリ判定部１１２を備えていたが、実施の形態２の情報処理装置２２０のアプリ特定部２０６は、検証部であるアプリ判定部を備えてない。さ

らに、実施の形態２のアプリ特定部２０６は、通信部２１２を新たに備えている。

[0160] さらに、実施の形態２の情報処理装置２２０は、ネットワーク２２２を介して、アプリ判定サーバ２２１に接続している。アプリ判定サーバ２２１は、検証部であるアプリ判定部２２３を備える。

[0161] また、実施の形態１と実施の形態２の動作の違いは以下の通りである。

[0162] 実施の形態１では、認証子生成部１１１が生成したハッシュ値（認証子）を、アプリ判定部１１２が、参照ハッシュ値（認証子）と比較・判定していた。

[0163] それに対して、実施の形態２では、認証子生成部２１１が生成したハッシュ値（認証子）を、通信部２１２が、図示されていないネットワーク機能を利用して、ネットワーク２２２を介して、アプリ判定サーバ２２１に送付する。アプリ判定サーバ２２１のアプリ判定部２２３は、送付されたハッシュ値（認証子）と、予め保持しているハッシュ値（認証子）とを、比較・判定することで、正当なアプリケーションであるか否かを判定する。

[0164] 上記の差異以外は、実施の形態１と実施の形態２は同一であるため、説明は省略する。

[0165] 本実施の形態２は、アプリ判定サーバでアプリケーションが正当であるか否かを判定する。そのため、実施の形態１とは異なり、アプリ判定ステップで使用するための予め保持するハッシュ値（認証子）を、情報処理装置２２０で保持する必要がない。従って、情報処理装置２２０の記憶領域を削減する事が出来るという効果がある。

[0166] （実施の形態３）

図１２は、本発明の実施の形態３に関わる情報処理装置のソフトウェア構成を示すブロック図である。

[0167] 図１３は、本発明の実施の形態３に関わる情報処理装置とアプリ判定部とサービス提供サーバがネットワーク接続された構成を示す図である。

[0168] 図１４は、本発明の実施の形態３に関わるデバイスアクセス制御のシーケ

ンスを示す図である。

[0169] 実施の形態１の情報処理装置１２０と実施の形態３の情報処理装置２５０との構成の差異は以下の通りである。

[0170] 実施の形態１と実施の形態３とのハードウェア構成の差異は、セキュアデバイスは、ネットワークインターフェースであることである。そして、前述のネットワークインターフェースを制御するデバイスドライバは、ネットワークインターフェースドライバ２３５である。

[0171] 実施の形態１の情報処理装置１２０では、アプリ特定部１０６が、検証部であるアプリ判定部１１２を備えていたが、実施の形態３の情報処理装置２５０のアプリ特定部２３６は、検証部であるアプリ判定部を備えてない。さらに、実施の形態３のアプリ特定部２３６は、通信部２４１を新たに備えている。さらに、実施の形態３のネットワークインターフェースドライバ２３５は、実行部であるデバイスアクセス制御部を備えていない。

[0172] さらに、実施の形態３の情報処理装置２５０と、アプリ判定サーバ２５１と、サービス提供サーバ２５２とは、ネットワーク２５３を介して互いに接続している。アプリ判定サーバ２５１は、検証部であるアプリ判定部２５４を備える。サービス提供サーバ２５２は、実行部としてのサービス提供部２５５とサービス提供判定部２５６を備える。

[0173] 実行部としてのサービス提供部２５５は、情報処理装置２５０に対して、コンテンツ配信などのサービスを提供する。

[0174] サービス提供判定部２５６は、情報処理装置２５０に対して、サービスを提供してよいか否かを判定する。

[0175] 図１４のシーケンスを用いて、情報処理装置２５０が、サービス提供サーバ２５２から、サービスを受けるステップを説明する。

[0176] まず、情報処理装置２５０で実施される、セキュアデバイス処理要求（Ｓ２００）、処理要求検出ステップ（Ｓ２０１）、対象アプリ抽出ステップ（Ｓ２０２）、対象アプリロックステップ（Ｓ２０３）、認証子生成ステップ（Ｓ２０４）、対象アプリロック解除ステップ（Ｓ２０９）は、実施の形態

１の各ステップと同一の処理内容のため、説明を省略する。

[0177] 認証子送信ステップ（Ｓ２０５）では、通信部２４１が、生成されたハッシュ値（認証子）を、ネットワーク２５３を介して、アプリ判定サーバ２５１に送付する。アプリ判定サーバ２５１のアプリ判定部２５４は、送付されたハッシュ値（認証子）と、予め保持しているハッシュ値（認証子）とを、比較・判定することで、正当なアプリケーションであるか否かを判定する。そして、アプリ判定部２５４は、サービス提供サーバ２５２に、ネットワーク２５３を介して、前述の判定結果を送付する（Ｓ２０６）。

[0178] サービス提供サーバ２５２のサービス提供判定部２５６は、送付された判定結果を受信する。

[0179] そして、サービス提供判定部２５６は、判定結果が正当なアプリケーションである場合には（Ｓ２０７）、サービス提供部２５５に、情報処理装置２５０に対して、サービスを提供するように指示する。サービスを提供するように指示されたサービス提供部２５５は、情報処理装置２５０に、ネットワーク２５３を介して、サービスを提供する（Ｓ２０８）。

[0180] また、サービス提供判定部２５６は、判定結果が不正なアプリケーションである場合には（Ｓ２０７）、情報処理装置２５０に対して、要求失敗であることを示す情報を通知する（Ｓ２０８）。

[0181] なお、アプリ判定サーバ２５１と、サービス提供サーバ２５２は、同一のサーバであっても良い。

[0182] なお、アプリ判定サーバ２５１と、サービス提供サーバ２５２は、情報処理装置２５０が接続されてない専用ネットワークで接続されていても良い。専用ネットワークで、アプリ判定サーバ２５１とサービス提供サーバ２５２とが接続されている場合には、アプリ判定サーバ２５１は、判定結果を専用ネットワークを介して、サービス提供サーバ２５２に通知する。

[0183] 上記の差異以外は、実施の形態１と実施の形態３は同一であるため、説明は省略する。

[0184] 実施の形態３では、サービス提供サーバが、情報処理装置に対してサービ

スを提供するか否かを判定する。そのため、ネットワークを介して、サービス提供者がソフトウェアを確認することが出来るという効果がある。

[0185] （実施の形態４）

図１５は、本発明の実施の形態４に関わる情報処理装置のソフトウェア構成を示すブロック図である。

[0186] 図１６は、本発明の実施の形態４に関わるデバイスアクセス制御のシーケンスを示す図である。

[0187] 実施の形態１の情報処理装置１２０と実施の形態４の情報処理装置との構成の差異は以下の通りである。

[0188] 実施の形態１の情報処理装置１２０では、セキュアデバイスドライバ１０５が、検出部としてのデバイスアクセス要求判定部１０９と、実行部としてのデバイスアクセス制御部１１０とを備えていたが、実施の形態４のセキュアデバイスドライバ２６５は、検出部としてのデバイスアクセス要求判定部と実行部としてのデバイスアクセス制御部とを備えていない。さらに、実施の形態４のセキュアＶＭＭ２６０は、検出部としてのデバイスアクセス要求判定部２６９と、実行部としてのデバイスアクセス制御部２７０とを備えている。

[0189] 図１６のシーケンスを用いて、実施の形態４の情報処理装置が、正当なアプリケーションのみに対して、セキュアデバイスをアクセスさせるステップを説明する。

[0190] 実施の形態１では、処理要求検出ステップ（Ｓ１０１）とデバイス処理判定ステップ（Ｓ１０６）とが、セキュアデバイスドライバ１０５で実現されていた。それに対して、実施の形態４では、処理要求検出ステップ（Ｓ２１１）とデバイス処理判定ステップ（Ｓ２１６）とが、セキュアＶＭＭ２６０で実現される。

[0191] 上記の差異以外は、実施の形態１と実施の形態４は同一であるため、説明は省略する。

[0192] 実施の形態４は、実施の形態１とは異なり、デバイスアクセス要求判定部

２６９とデバイスアクセス制御部２７０が、セキュアＶＭＭ２６０内部に存在し、セキュアデバイスドライバ２６５内部に存在しない。従って、セキュアデバイスドライバを改変することなしに、実施の形態４の情報処理装置で動作させることが出来るという効果がある。

[0193] （実施の形態５）

図１７は、本発明の実施の形態５に関わる情報処理装置のソフトウェア構成を示すブロック図である。

[0194] 図１８は、本発明の実施の形態５に関わるデバイスアクセス制御のシーケンスを示す図である。

[0195] 実施の形態１の情報処理装置１２０と実施の形態５の情報処理装置との構成の差異は以下の通りである。

[0196] 実施の形態１の情報処理装置１２０では、アプリ特定部１０６が、検証部としての認証子生成部１１１を備えていたが、実施の形態５のアプリ特定部２８６は、検証部としての認証子生成部を備えていない。さらに、実施の形態５のセキュアＶＭＭ２８０は、検証部としての認証子生成部２８９を備えている。

[0197] 図１８のシーケンスを用いて、実施の形態５の情報処理装置が、正当なアプリケーションのみに対して、セキュアデバイスをアクセスさせるステップを説明する。

[0198] 実施の形態１では、認証子生成ステップ（Ｓ１０４）が、アプリ特定部１０６で実現されていた。それに対して、実施の形態５では、認証子生成ステップ（Ｓ２２４）が、セキュアＶＭＭ２８０で実現される。

[0199] 上記の差異以外は、実施の形態１と実施の形態５は同一であるため、説明は省略する。

[0200] 実施の形態５では、実施の形態１とは異なり、認証子生成部２８９が、セキュアＶＭＭ２８０内部に存在し、アプリ特定部２８６内部に存在しない。そのため、動作アプリ格納メモリ特定部２８７から認証子生成部２８９への情報通知が、同一モジュール（セキュアＶＭＭ２８０）内部で実現できる。

従って、動作アプリ格納メモリ特定部２８７から認証子生成部２８９への情報通知が、より高速に出来るという効果がある。

[0201] （その他変形例）

（１）上記の実施の形態で、処理要求検出ステップにおいて、処理要求自体を検出するのではなく、要求のコマンド種別や、データの処理内容を参照することで処理要求が行われているか否かを判断して検出するとしても良い。

[0202] （２）上記の実施の形態で、処理要求検出ステップが、デバイス初期化の操作のみに対して検出操作を行うとしてもよい。

[0203] （３）上記の実施の形態で、処理要求検出ステップの検出を行うか否かを、乱数に基づいて、ランダムに決定するとしても良い。

[0204] （４）上記の実施の形態で、処理要求検出ステップの検出を行うか否かを、デバイスアクセス回数に基づいて切り替えるとしても良い。例えば、セキュアデバイスドライバに対して、１０回のアクセスを行った場合には、検出するという操作を行ってもよい。

[0205] （５）上記の実施の形態で、認証子生成ステップのハッシュ値の生成において、ＳＨＡ１以外の一方向性関数を用いてもよい。例えば、ＭＤ５や、ＳＨＡ２５６、ＡＥＳ、ＤＥＳを用いても良い。

[0206] （６）上記の実施の形態で、認証子生成ステップのハッシュ値の生成において、論理アドレス空間の一部のみを用いて、ハッシュ値を生成しても良い。例えば、アプリケーションのコード領域のみのハッシュ値を生成しても良い。

[0207] （７）上記の実施の形態で、認証子生成ステップのハッシュ値の生成において、複数個のハッシュ値を生成しても良い。例えば、論理メモリ空間を分割して、分割した領域毎にハッシュ値を生成しても良い。

[0208] （８）上記の実施の形態で、対象アプリロックステップのページテーブルの情報をバックアップする場合に、一部の情報のみをバックアップしても良い。

[0209] （９）上記の実施の形態で、アプリ判定部は、特定のアプリケーションライセンスを備えたアプリケーションのみを不正アプリケーションであると判定しても良い。

[0210] （１０）上記の実施の形態で、ＣＰＵが、保護モードと通常モードを備えるＣＰＵであってもよい。さらに、保護モードのＣＰＵのみが、保護メモリにアクセス可能であってもよい。

[0211] （１１）上記の実施の形態で、保護メモリとセキュアデバイスは、保護メモリに格納されたソフトウェアのみがアクセス可能となるように制御されるが、その手段は、ハードウェアによって実現してもよい。例えば、保護メモリ上のプログラムが動作しているときのみ、ＣＰＵから、保護メモリとセキュアデバイスへアクセス可能になるようにバスが制御されていてもよい。

[0212] （１２）上記の実施の形態で、通常メモリと保護メモリとが、同一のメモリであってもよい。

[0213] （１３）上記の実施の形態で、不揮発性記憶装置が、汎用ＯＳを格納していてもよい。その場合は、ＢＩＯＳ（Ｂａｓｉｃ Ｉｎｐｕｔ Ｏｕｔｐｕｔ Ｓｙｓｔｅｍ）や、ＩＰＬ（Ｉｎｉｔｉａｌ Ｐｒｏｇｒａｍ Ｌｏａｄｅｒ）と呼ばれる特別なファームウエア（プログラム）によって、汎用ＯＳを通常メモリ上にロードさせる。

[0214] （１４）上記の実施の形態で、不揮発性記憶装置が、セキュアデバイスドライバや、アプリ特定部や、管理専用ＯＳや、セキュアＶＭＭを格納していてもよい。その場合には、ＡＥＳ暗号などの秘密鍵暗号方式や、ＲＳＡ暗号などの非対称鍵暗号方式などの暗号アルゴリズムを用いて、セキュアデバイスドライバや、アプリ特定部や、管理専用ＯＳや、セキュアＶＭＭは暗号化されて格納されている。そして、各モジュールは、復号されて保護メモリ上にロードされ、実行される。

[0215] （１５）上記の実施の形態では、セキュアＶＭＭが通常メモリに格納されていてもよい。その場合には、保護メモリに格納されている図示されていない改ざん検出プログラムが、セキュアＶＭＭの改ざん検出を行ってもよい。

さらに、前述のセキュアＶＭＭの改ざん検出は、セキュアＶＭＭを通常メモリにロードする場合に行ってもよく、定期的に改ざん検出をおこなってもよく、乱数などに基づいて不定期に行ってもよく、何らかのトリガに基づいて行ってもよい。

[0216] （１６）上記の実施の形態では、セキュアＶＭＭが通常メモリに格納されていてもよい。その場合には、情報処理装置内部の読み込み専用記憶装置（ＲＯＭ）に格納されている図示されていない改ざん検出プログラムが、セキュアＶＭＭの改ざん検出を行ってもよい。さらに、前述のセキャアＶＭＭの改ざん検出は、セキュアＶＭＭを通常メモリにロードする場合に行ってもよく、定期的に改ざん検出をおこなってもよく、乱数などに基づいて不定期に行ってもよく、何らかのトリガに基づいて行ってもよい。

[0217] （１７）上記の実施の形態では、ＣＰＵの特権状態をＣＰＵのリングの機構を用いて実現したが、それ以外の方法であってもよい。例えば、完全仮想化をサポートしたＣＰＵの仮想化ドメイン（管理ドメインと汎用ドメイン）の機構を利用してもよい。

[0218] （１８）上記の実施の形態では、汎用ＯＳが、アプリケーションのページテーブルを管理していたが、それ以外の方法であってもよい。例えば、ＯＳ仮想化技術のシャドー・ページングを利用して、セキュアＶＭＭがページテーブルを管理してもよい。

[0219] また、上記の実施の形態では、汎用ＯＳが管理するアプリケーションごとのページテーブルを、セキュアＶＭＭがカレントページテーブルとして参照する構成を取っていた。より具体的には、カレントページテーブルを指すポインタを、汎用ＯＳが管理するページテーブルのうちの現在処理中のアプリケーションに対応するページテーブルに繋ぐ構成を取っていた。しかし、これに限られるものではない。例えば、上述のシャドー・ページングを使う場合は、動作させるアプリケーションの切り替えが起こるたびに、セキュアＶＭＭ自身が、汎用ＯＳが管理するページテーブルのコピーを作る。この場合、メモリアクセスの制御は、セキュアＶＭＭが保持するページテーブルに基

づいて行われるので、セキュアＶＭＭは、自身が複製したページテーブルに対して、上記の実施の形態におけるカレントページテーブルと同様の処理を行うとすればよい。

[0220] （１９）上記の実施の形態２と実施の形態３では、情報処理装置からアプリ判定サーバに対して、ハッシュ値（認証子）と共に、情報処理装置を識別する情報を送付してもよい。

[0221] （２０）上記の実施の形態２と実施の形態３では、情報処理装置とアプリ判定サーバとで、安全な通信路を用いても良い。例えば、ＳＳＬを利用しても良い。

[0222] （２１）上記の実施の形態２と実施の形態３では、情報処理装置からアプリ判定サーバに対して送付する情報を、電子署名を用いて保護してもよい。例えば、ＴＣＧ（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ）のＴＰＭ（Ｔｒｕｓｔｅｄ　Ｐｌａｔｆｏｒｍ　Ｍｏｄｕｌｅ）を用いて、送付する情報に対して電子署名を作成し、アプリ判定サーバに電子署名を送付してもよい。

[0223] （２２）上記の実施の形態２と実施の形態３では、情報処理装置とアプリ判定サーバとで、チャレンジ・レスポンス処理を行い、相互認証を行ってもよい。

[0224] （２３）上記の実施の形態では、ＣＰＵは、自身の特権状態よりもレベルの低い特権情報に対応するページテーブルのエントリは全てアクセスできるとしていたが、これに限られるものではない。例えば、特権状態と特権情報とを１対１に対応させ、リング３の特権状態の時はリング３の特権情報を持つエントリにしかアクセスできないとしてもよい。

[0225] （２４）上記の実施の形態で述べた構成要素については、その一部または全てを実現可能な範囲でソフトウェアとして実装してもよい。この場合、集積回路上に乗せなくてはならないハードウェアの量を抑えることができるので、より集積度を向上させることができる。

[0226] （２５）上記の実施の形態で述べた構成要素については、その一部または

全てを実現可能な範囲でハードウェアとして実装してもよい。この場合、上記の構成要素をソフトウェアで実装するよりも処理を高速化することができる。このような実装は、特に退避処理や復帰処理等、ユーザの利便性のために高速化が求められる処理などにおいて有用である。

[0227] （２６）システムＬＳＩは集積度の違いにより、ＩＣ、ＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもあるが、システムＬＳＩを上記のいずれの集積度で実現した場合も本発明に含まれることは言うまでもない。また、ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用しても良い。

[0228] さらには、半導体技術の進歩または派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて構成要素の集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

[0229] （２７）また、本発明は、前記コンピュータプログラムまたは前記ディジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙＤｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記ディジタル信号であるとしてもよい。

[0230] （２８）これらの実施の形態および変形例の組合せであってもよい。

産業上の利用可能性

[0231] 本発明にかかるセキュアデバイスに対するアクセス制御を行う手法は、アプリケーションが格納されている論理メモリ空間をロックし、ハッシュ値を生成・判定することによって、アプリケーションの差し替えによる不正アプリケーションのデバイスアクセスを防止するという効果を有する。そのため、セキュアデバイスを処理するデータ処理において、不正アプリケーションの動作を防止させるという効果がある。

請求の範囲

[1] 所定のデバイスにアクセスする所定のアプリケーションをワークエリア上で動作させる仮想マシンと、

前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、

前記所定のアプリケーションの正当性を検証する検証部と、

前記仮想マシン、前記検証部及び前記検出部を管理し、前記ワークエリア上で動作する所定のアプリケーションを書き換え可能に管理する仮想マシンモニタと、を具備し、

前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、

前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直してその旨を前記検証部に通知し、

前記検証部は前記仮想マシンモニタからの通知を受けると前記所定のアプリケーションが正当であるか否かを判断することを特徴とする情報処理装置。

[2] 前記検証部が前記所定のアプリケーションが正当であると判断した場合、前記所定のアプリケーションを用いて所定のデバイスにアクセスする実行部を設けたことを特徴とする請求項１記載の情報処理装置。

[3] 前記仮想マシンモニタは、前記実行部が前記所定のアプリケーションを用いた所定のデバイスへのアクセスを終了した後、前記所定のアプリケーションを書換え可能なものに管理を戻すことを特徴とする請求項２記載の情報処理装置。

[4] 前記仮想マシンモニタは、前記ワークエリアに前記所定のアプリケーションに対応する管理情報を管理し、前記管理情報は前記管理情報を書換える権限を有する主体を示す特権情報を含み、前記所定のアプリケーションの書換え可能な主体が前記仮想マシンを含む旨を前記特権情報が示している場合、前記所定のアプリケーションの書換え可能な主体から前記仮想マシンを排除

するように前記特権情報を書き換えることで、前記所定のアプリケーションを書換え不可能なものと管理することを特徴とする請求項１記載の情報処理装置。

[5] 前記仮想マシンモニタは、前記所定のアプリケーションの書換え可能な主体を前記仮想マシン及び前記仮想マシンモニタを含む情報から、前記所定のアプリケーションの書換え可能な主体を前記仮想マシンモニタに制限する情報に前記特権情報を書き換えることで、前記所定のアプリケーションの書換え可能な主体から前記仮想マシンを排除することを特徴とする請求項４記載の情報処理装置。

[6] 前記所定のデバイスは、ＳＤカードであることを特徴とする請求項１記載の情報処理装置。

[7] 前記所定のデバイスは、前記情報処理装置にコンテンツを提供する外部のコンテンツサーバであることを特徴とする請求項１記載の情報処理装置。

[8] 所定のデバイスにアクセスする前記所定のアプリケーションをワークエリア上で動作させる仮想マシンと、

前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、

前記仮想マシン及び前記検出部を管理し、前記ワークエリア上で動作する所定のアプリケーションを書き換え可能に管理する仮想マシンモニタと、を具備し、

前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、

前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直して、その旨を検証部を備える外部装置に通知し、前記外部装置の検証部に前記所定のアプリケーションが正当であるか否かの判断を行わせることを特徴とする情報処理装置。

[9] 所定のデバイスにアクセスする所定のアプリケーションをワークエリア上で動作させる仮想マシンと、

前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、

前記仮想マシン及び前記検出部を管理し、前記ワークエリア上で動作する所定のアプリケーションを書き換え可能に管理する仮想マシンモニタと、

サービスを提供する実行部を備える外部装置と通信する通信部と、を具備し、

前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、

前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直し、

前記通信部は、前記所定のアプリケーションが書換え不可能なものと管理し直された後に正当なものであると判断された場合に、前記外部装置の実行部から前記サービスの提供を受けることを特徴とする情報処理装置。

[10] 所定のデバイスにアクセスする所定のアプリケーションをワークエリア上で動作させる仮想マシンと、

前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、

前記所定のアプリケーションの正当性を検証する検証部と、

前記仮想マシン、前記検証部及び前記検出部を管理する仮想マシンモニタと、を具備した情報処理装置の制御方法であって、

前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、

前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直してその旨を前記検証部に通知し、

前記検証部は前記仮想マシンモニタからの通知を受けると前記所定のアプリケーションが正当であるか否かを判断することを特徴とする制御方法。

[11] 所定のデバイスにアクセスする所定のアプリケーションをワークエリア上で動作させる仮想マシンと、

前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、

前記所定のアプリケーションの正当性を検証する検証部と、

前記仮想マシン、前記検証部及び前記検出部を管理する仮想マシンモニタと、を具備した情報処理装置の制御プログラムであって、

前記検出部が前記アクセス要求を検出すると、その旨を前記仮想マシンモニタに通知するステップと、

前記仮想マシンモニタに、前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直させ、その旨を前記検証部に通知させるステップと、

前記仮想マシンモニタからの通知を受けた前記検証部に、前記所定のアプリケーションが正当であるか否かを判断させるステップとを含む

ことを特徴とする制御プログラム。

[12] 情報処理装置に用いられる集積回路であって、

所定のデバイスにアクセスする所定のアプリケーションをワークエリア上で動作させる仮想マシンと、

前記所定のアプリケーションを用いた所定のデバイスへのアクセス要求を前記仮想マシンから検出する検出部と、

前記所定のアプリケーションの正当性を検証する検証部と、

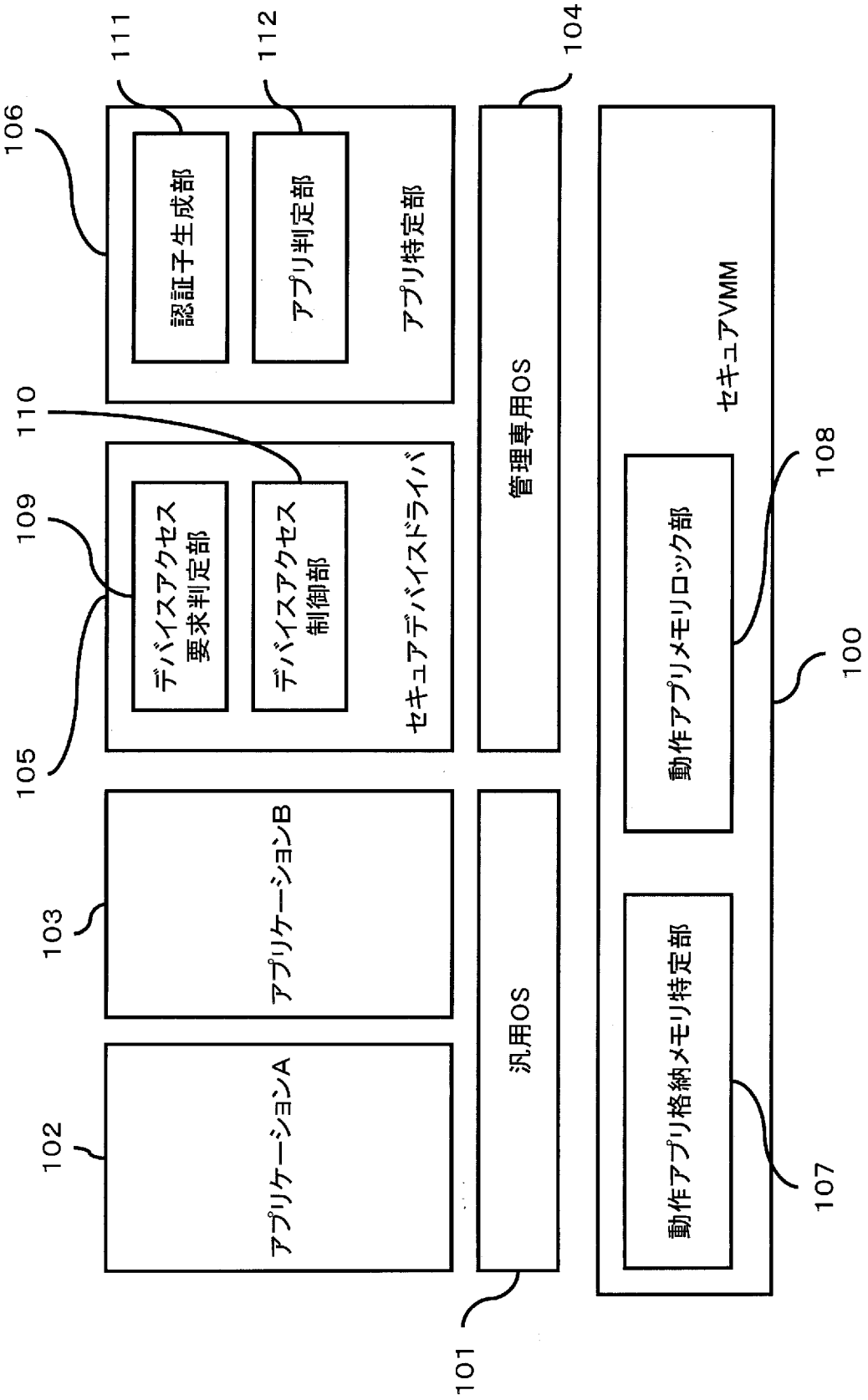
前記仮想マシン、前記検証部及び前記検出部を管理する仮想マシンモニタと、を具備し、

前記検出部は前記アクセス要求を検出するとその旨を前記仮想マシンモニタに通知し、

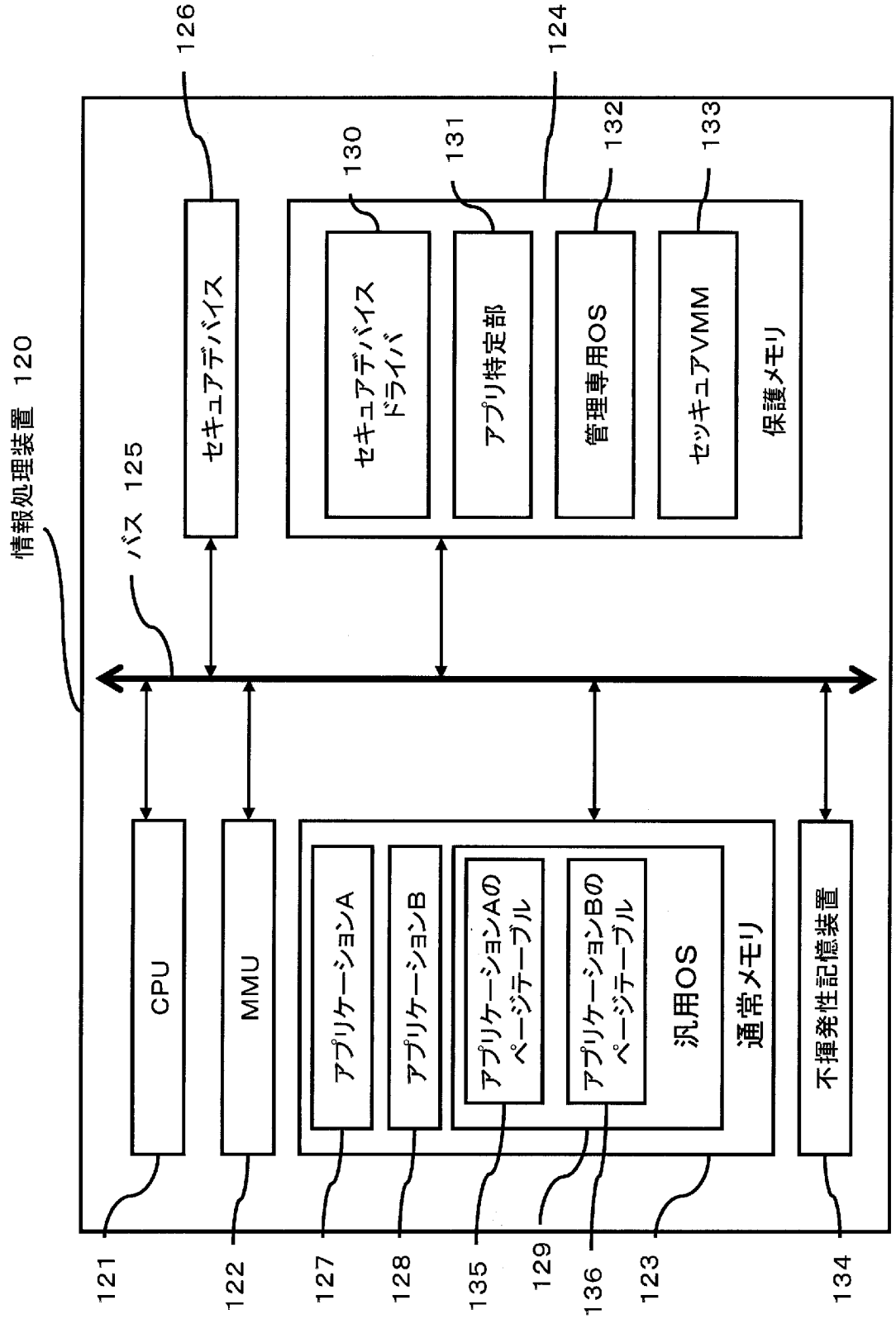
前記仮想マシンモニタは前記ワークエリア上の前記所定のアプリケーションを書換え不可能なものと管理し直してその旨を前記検証部に通知し、

前記検証部は前記仮想マシンモニタからの通知を受けると前記所定のアプリケーションが正当であるか否かを判断することを特徴とする集積回路。

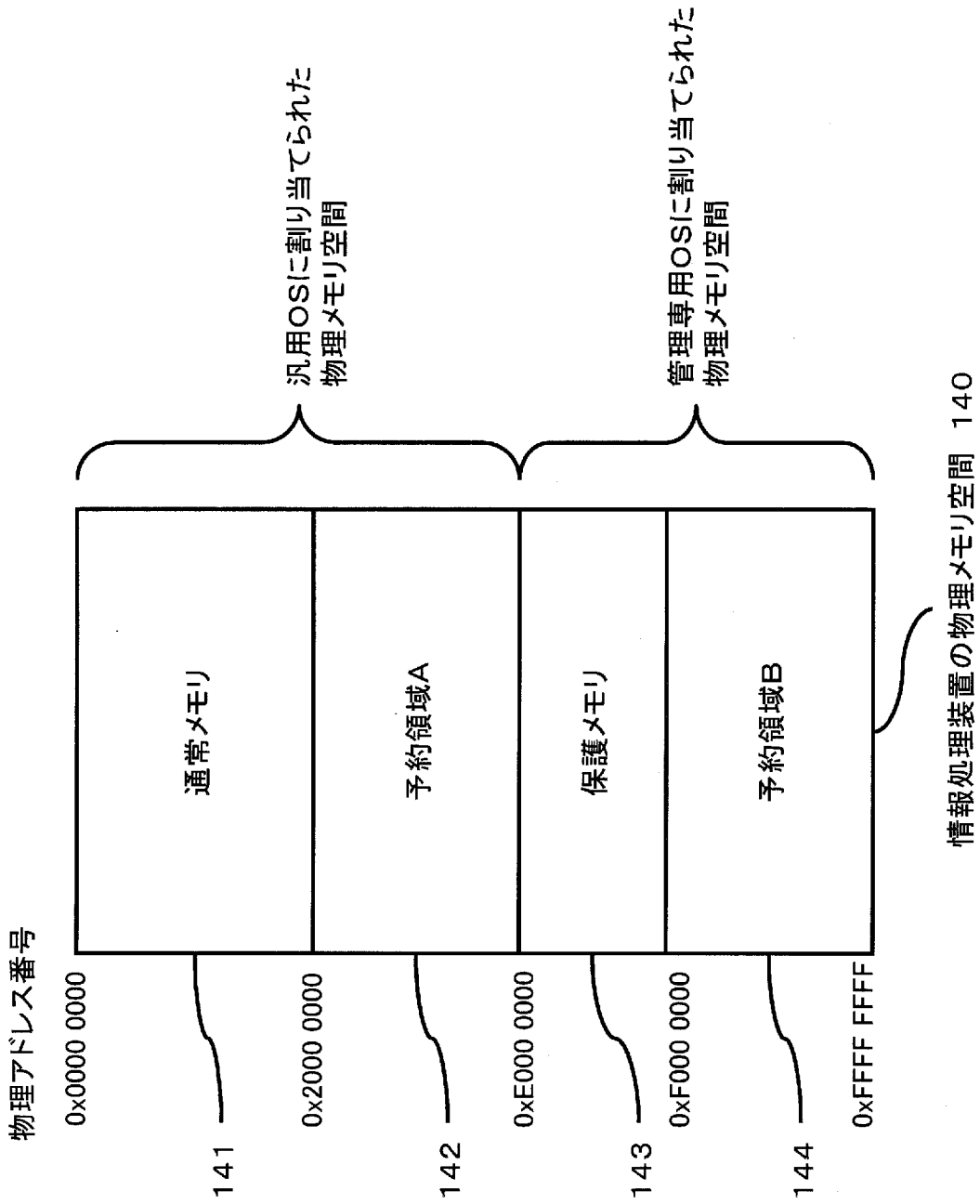
[図1]


101
102
アプリケーションA
103
アプリケーションB
汎用OS
105
109
デバイスアクセス要求判定部
110
デバイスアクセス制御部
セキュアデバイスドライバ
106
111
認証子生成部
112
アプリ判定部
アプリ特定部
104
管理専用OS
100
107
動作アプリ格納メモリ特定部
108
動作アプリメモリロック部
セキュアVMM

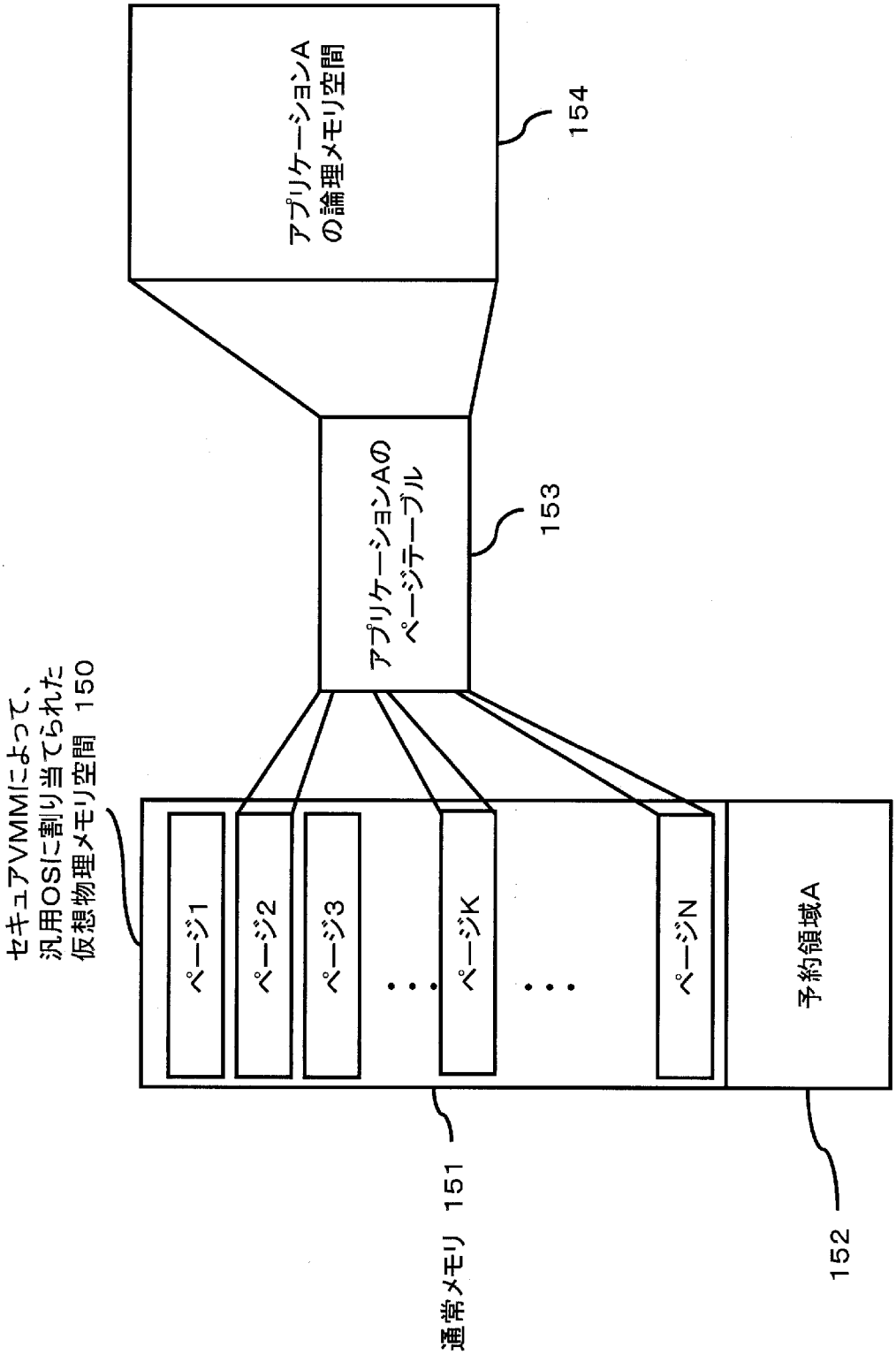
[図2]


情報処理装置 120
バス 125
126
セキュアデバイス
124
130
131
132
133
セキュアデバイス ドライバ
アプリ特定部
管理専用OS
セッキュアVMM
保護メモリ
CPU
MMU
アプリケーションA
アプリケーションB
アプリケーションAの ページテーブル
アプリケーションBの ページテーブル
汎用OS
通常メモリ
不揮発性記憶装置
121
122
127
128
135
129
136
123
134

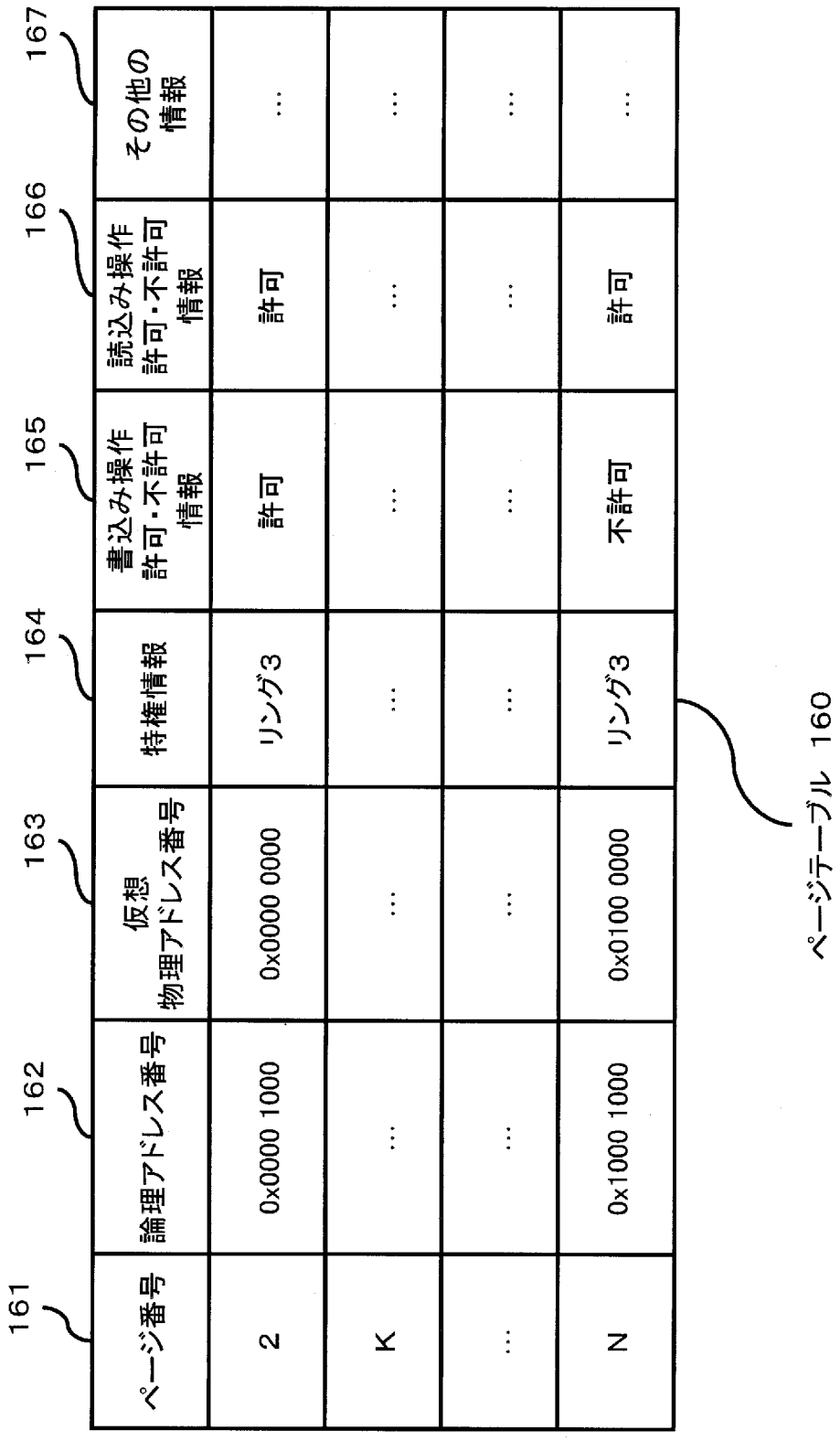
[図3]


物理アドレス番号
0x0000 0000
0x2000 0000
0xE000 0000
0xF000 0000
0xFFFF FFFF
141
142
143
144
通常メモリ
予約領域A
保護メモリ
予約領域B
汎用OSに割り当てられた
物理メモリ空間
管理専用OSに割り当てられた
物理メモリ空間
情報処理装置の物理メモリ空間 140

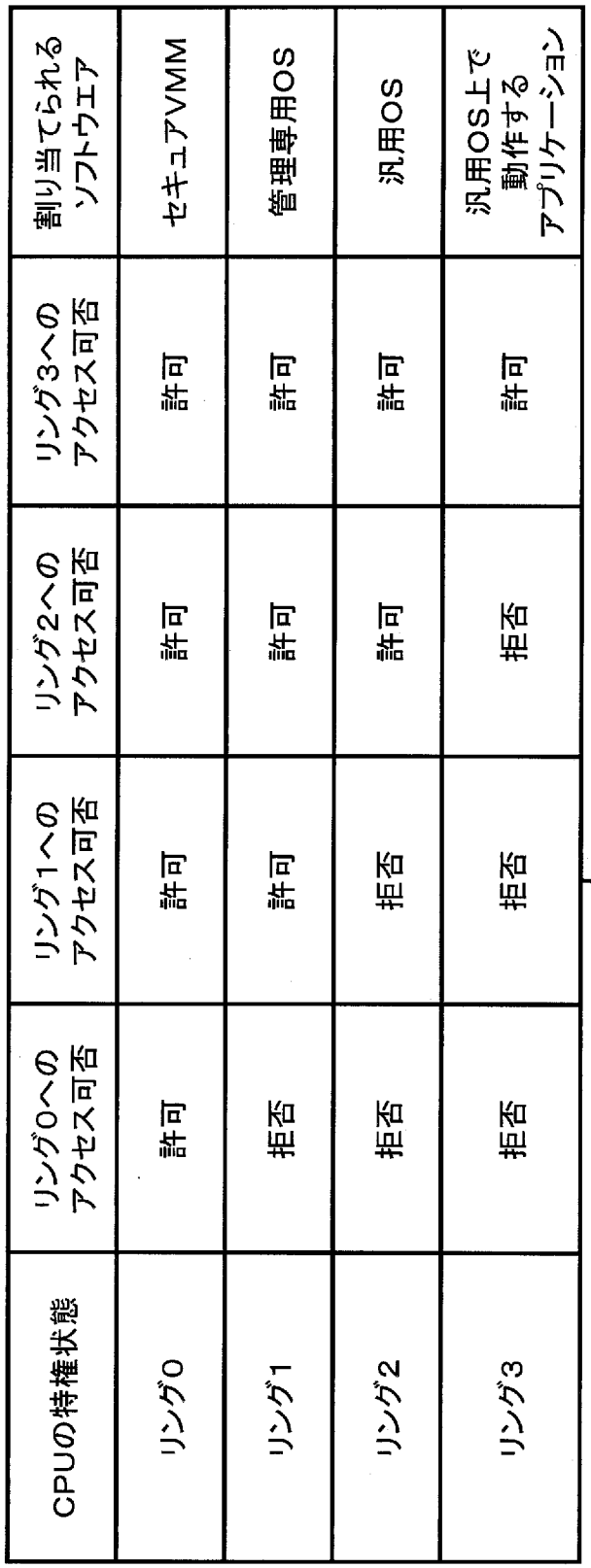
[図4]


アプリケーションAの論理メモリ空間
154
アプリケーションAのページテーブル
153
セキュアVMMによって、汎用OSに割り当てられた仮想物理メモリ空間 150
ページ1
ページ2
ページ3
ページK
ページN
予約領域A
通常メモリ 151
152

[図5]


161
162
163
164
165
166
167
ページ番号
論理アドレス番号
仮想物理アドレス番号
特権情報
書込み操作許可・不許可情報
読込み操作許可・不許可情報
その他の情報
2
0x0000 1000
0x0000 0000
リング3
許可
許可
…
K
…
…
…
…
…
…
…
…
…
…
…
…
…
N
0x1000 1000
0x0100 0000
リング3
不許可
許可
…
ページテーブル 160

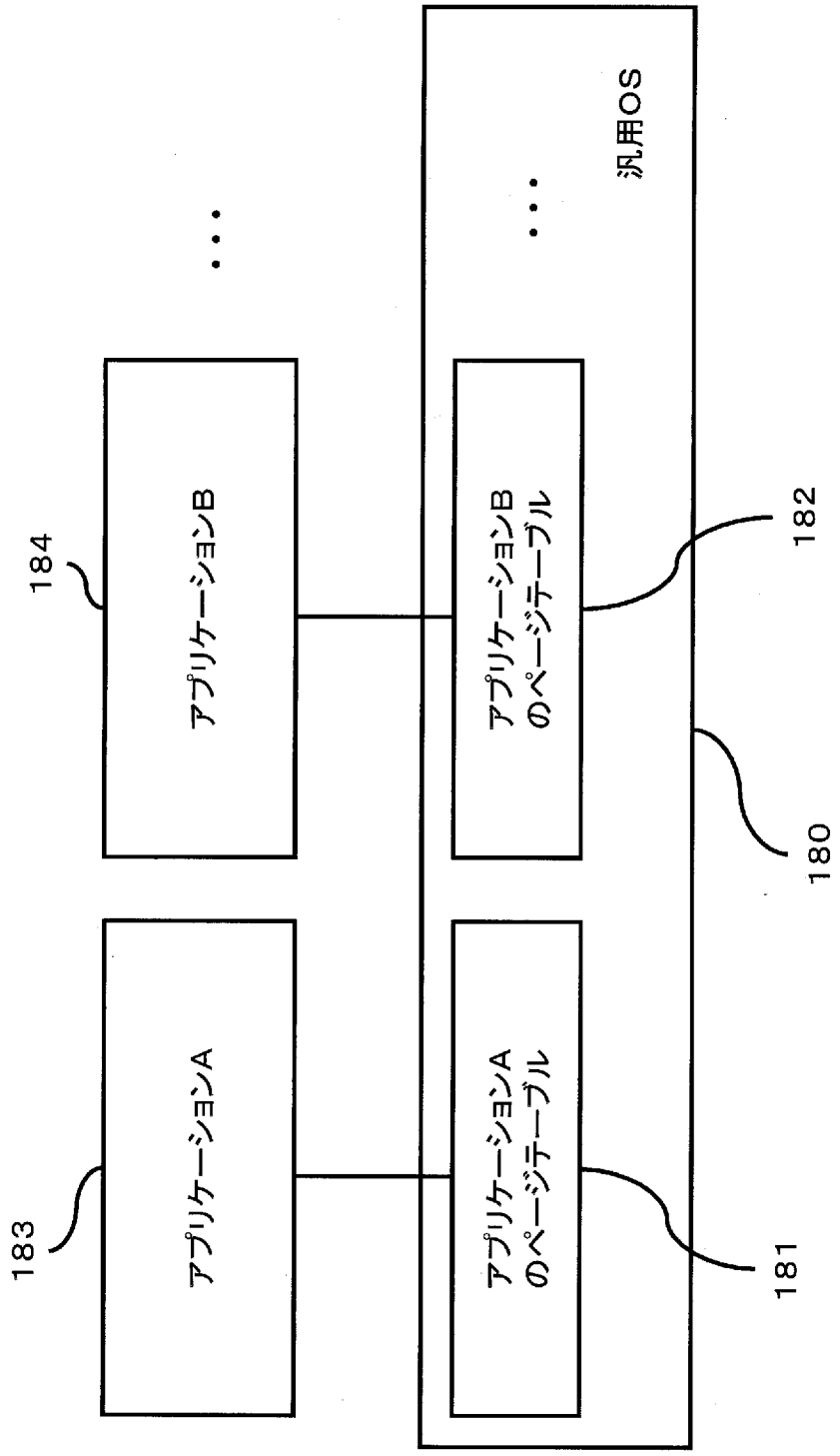
[図6]



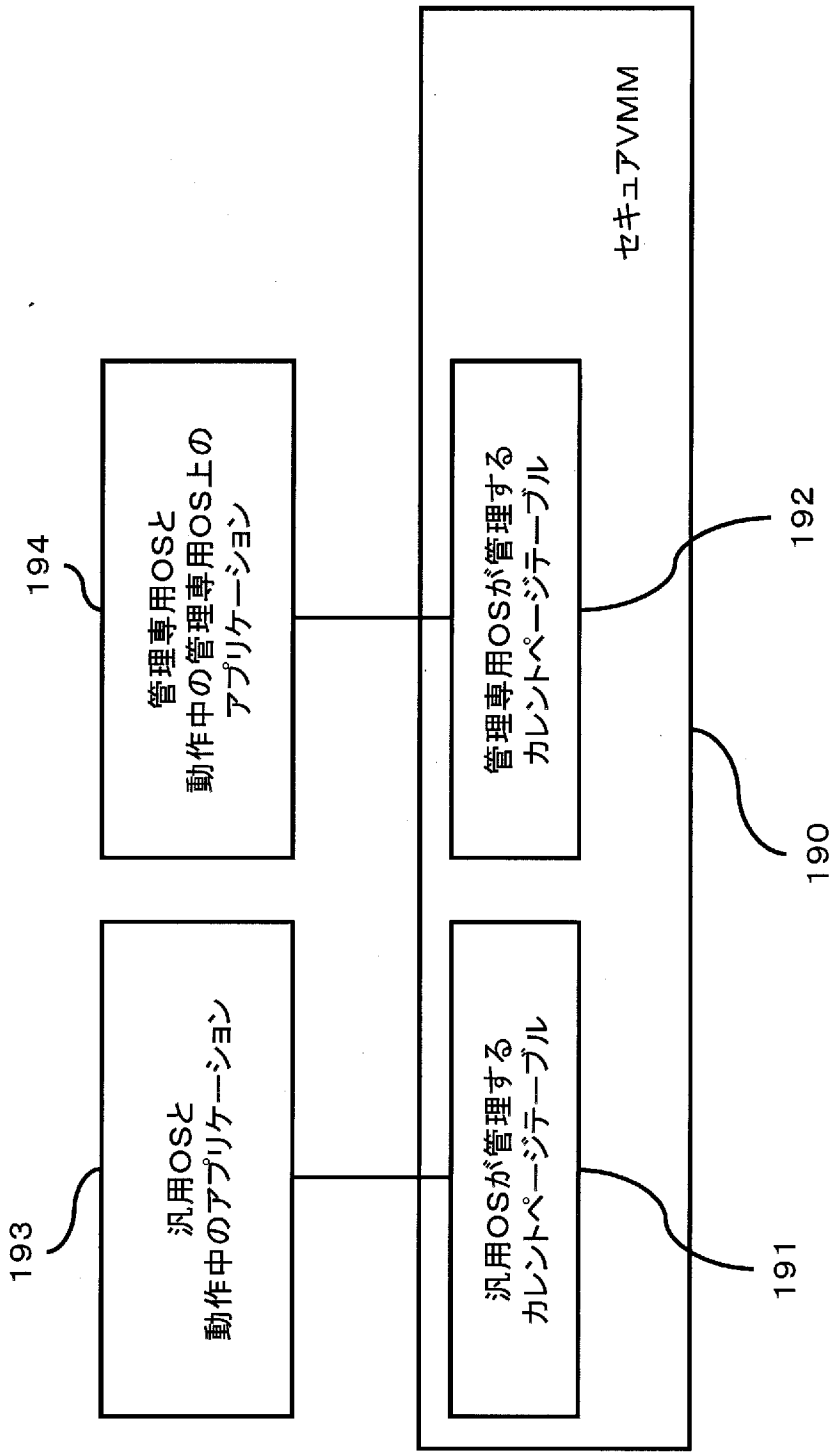
CPUの特権状態	リング0へのアクセス可否	リング1へのアクセス可否	リング2へのアクセス可否	リング3へのアクセス可否	割り当てられるソフトウエア
リング0	許可	許可	許可	許可	セキュアVMM
リング1	拒否	許可	許可	許可	管理専用OS
リング2	拒否	拒否	許可	許可	汎用OS
リング3	拒否	拒否	拒否	許可	汎用OS上で動作するアプリケーション

170

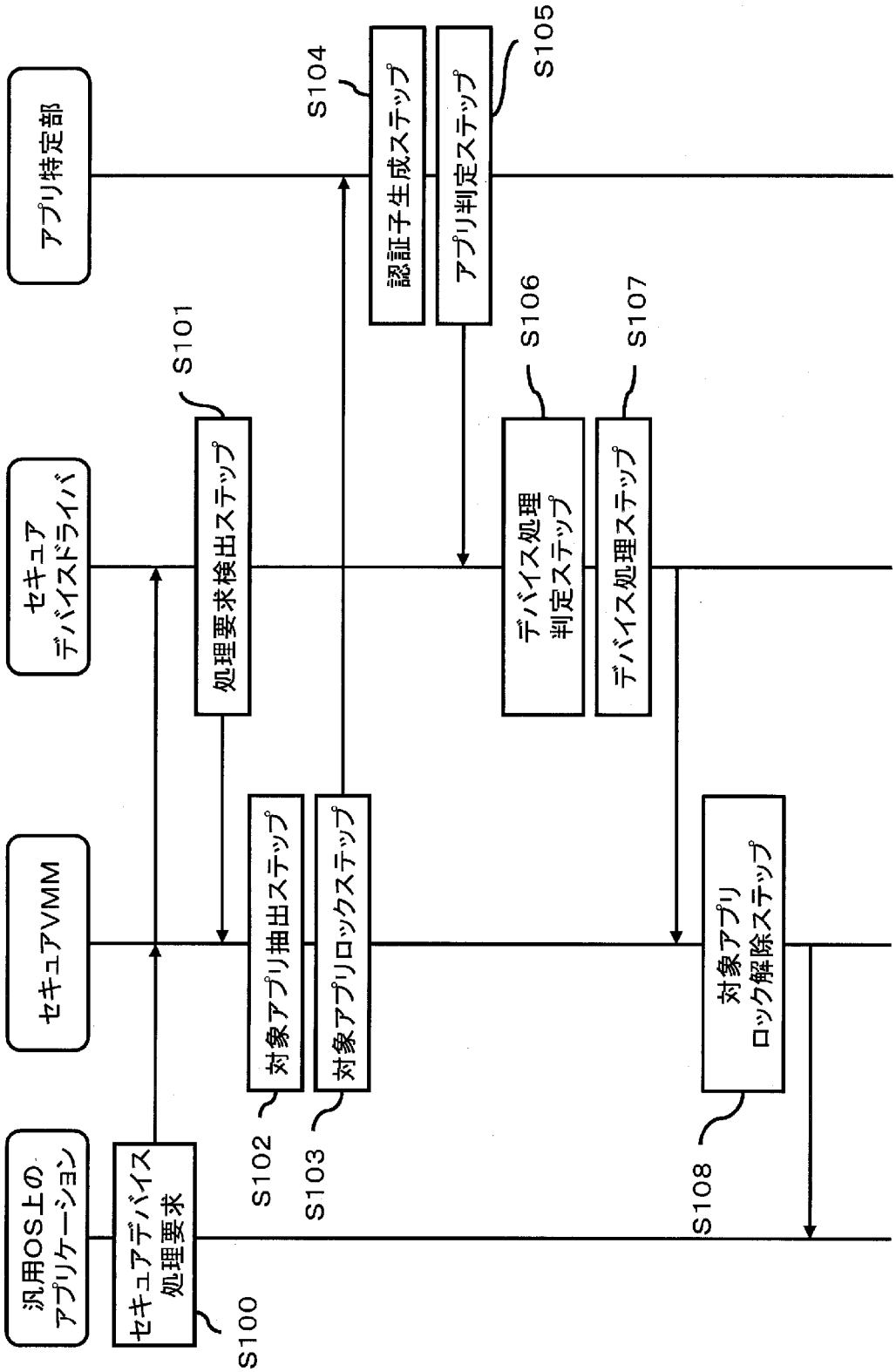
[図7]


汎用OS
アプリケーションB
アプリケーションA
アプリケーションBのページテーブル
アプリケーションAのページテーブル
180
181
182
183
184

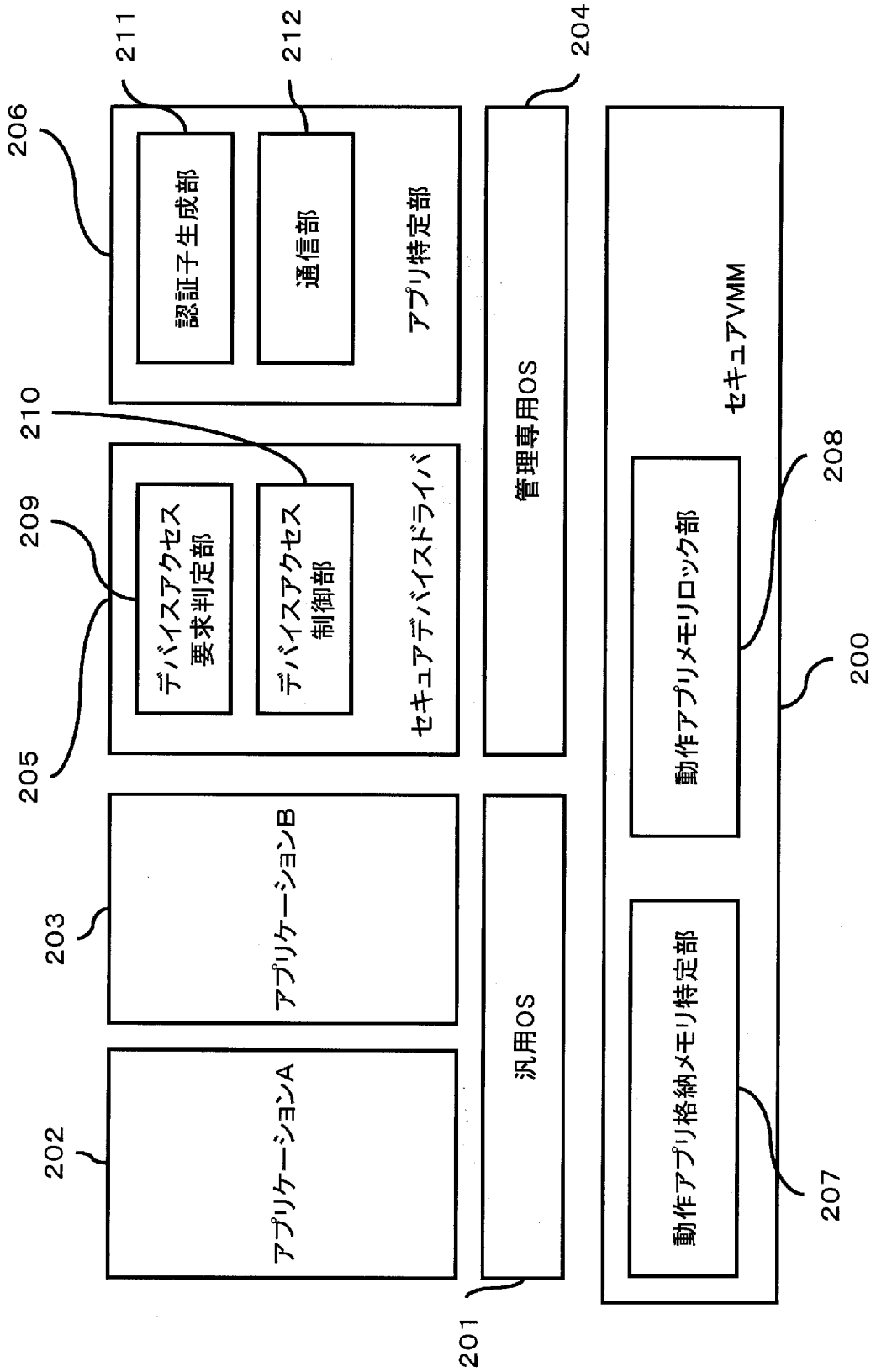
[図8]


セキュアVMM
管理専用OSと
動作中の管理専用OS上の
アプリケーション
194
管理専用OSが管理する
カレントページテーブル
192
190
汎用OSと
動作中のアプリケーション
193
汎用OSが管理する
カレントページテーブル
191

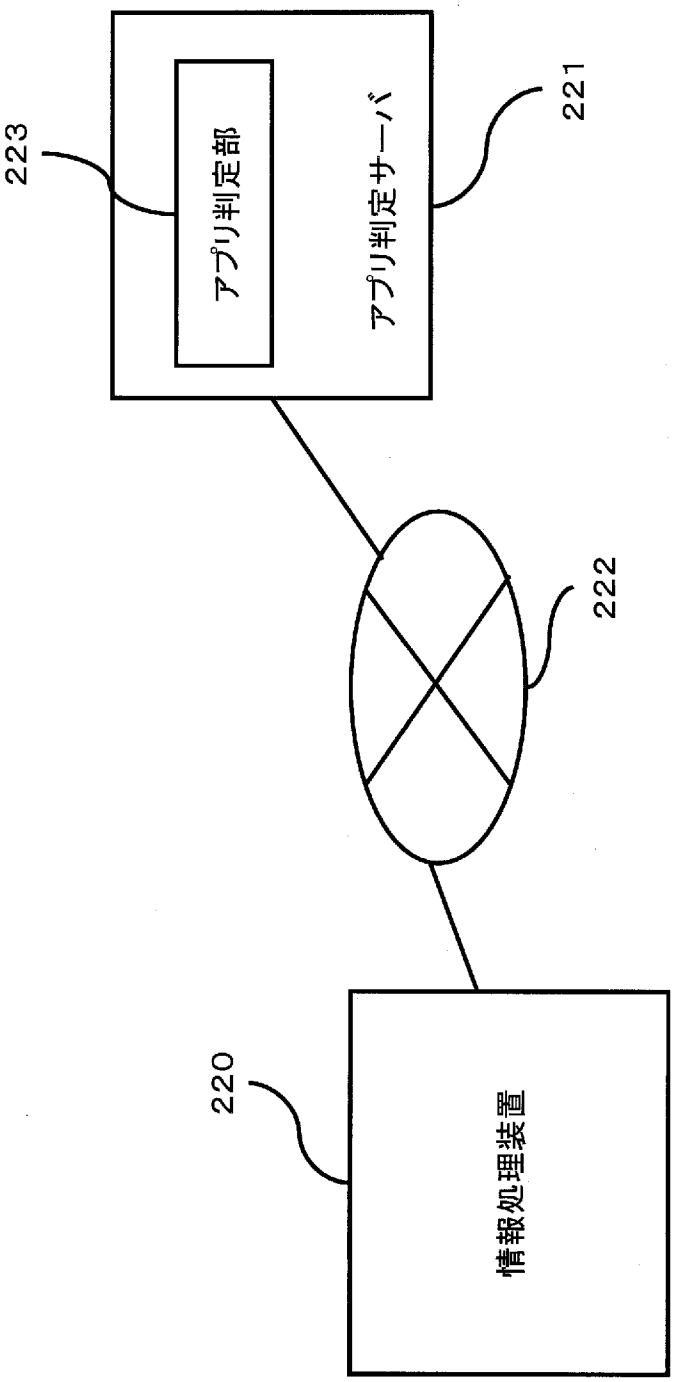
[図9]


汎用OS上の
アプリケーション
セキュアVMM
セキュア
デバイスドライバ
アプリ特定部
セキュアデバイス
処理要求
処理要求検出ステップ
対象アプリ抽出ステップ
対象アプリロックステップ
認証子生成ステップ
アプリ判定ステップ
デバイス処理
判定ステップ
デバイス処理ステップ
対象アプリ
ロック解除ステップ
S100
S101
S102
S103
S104
S105
S106
S107
S108

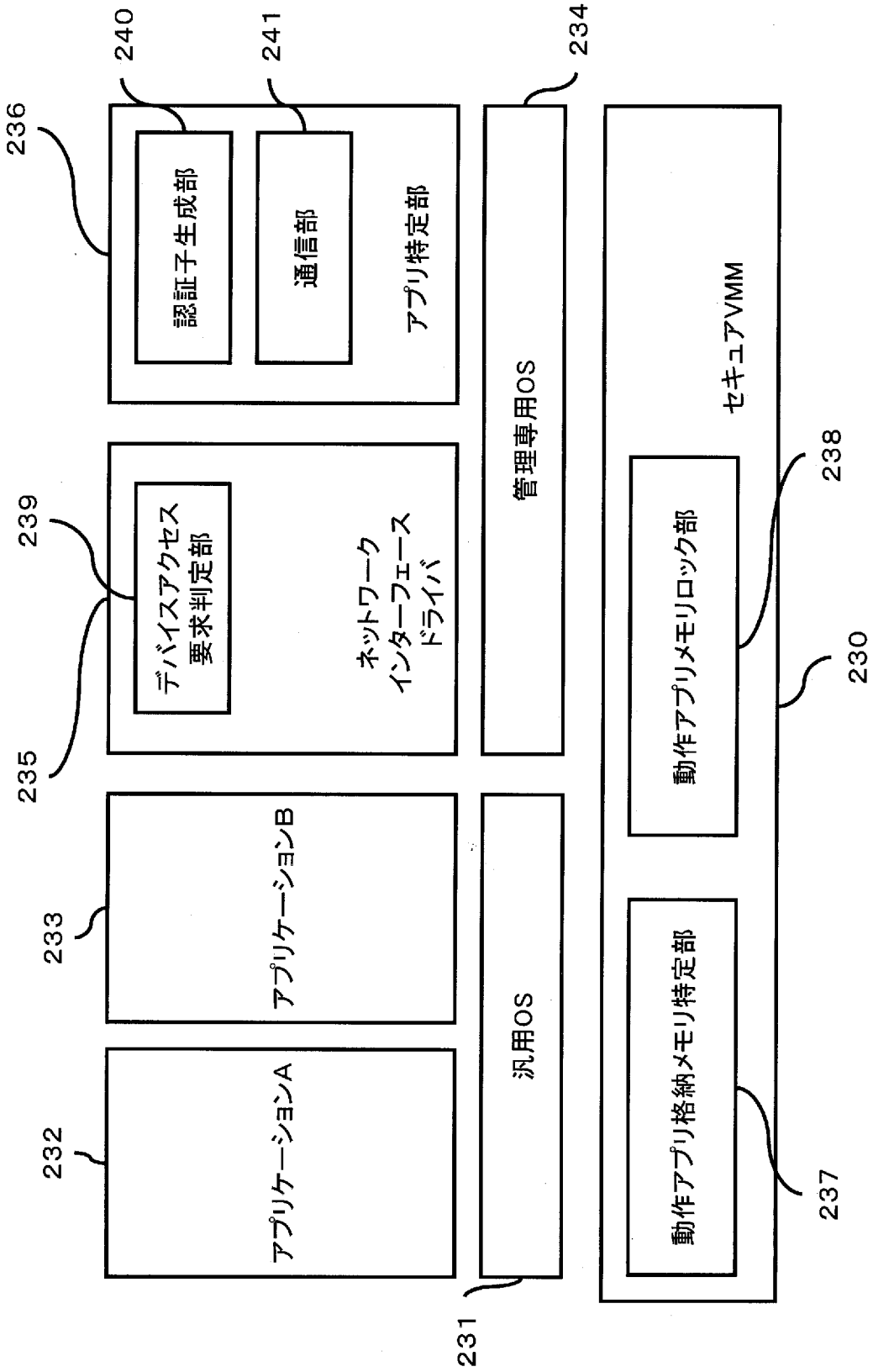
[図10]


211
212
204
206
認証子生成部
通信部
アプリ特定部
管理専用OS
セキュアVMM
210
209
デバイスアクセス
要求判定部
デバイスアクセス
制御部
セキュアデバイスドライバ
動作アプリメモリロック部
208
205
200
203
アプリケーションB
汎用OS
202
アプリケーションA
動作アプリ格納メモリ特定部
207
201

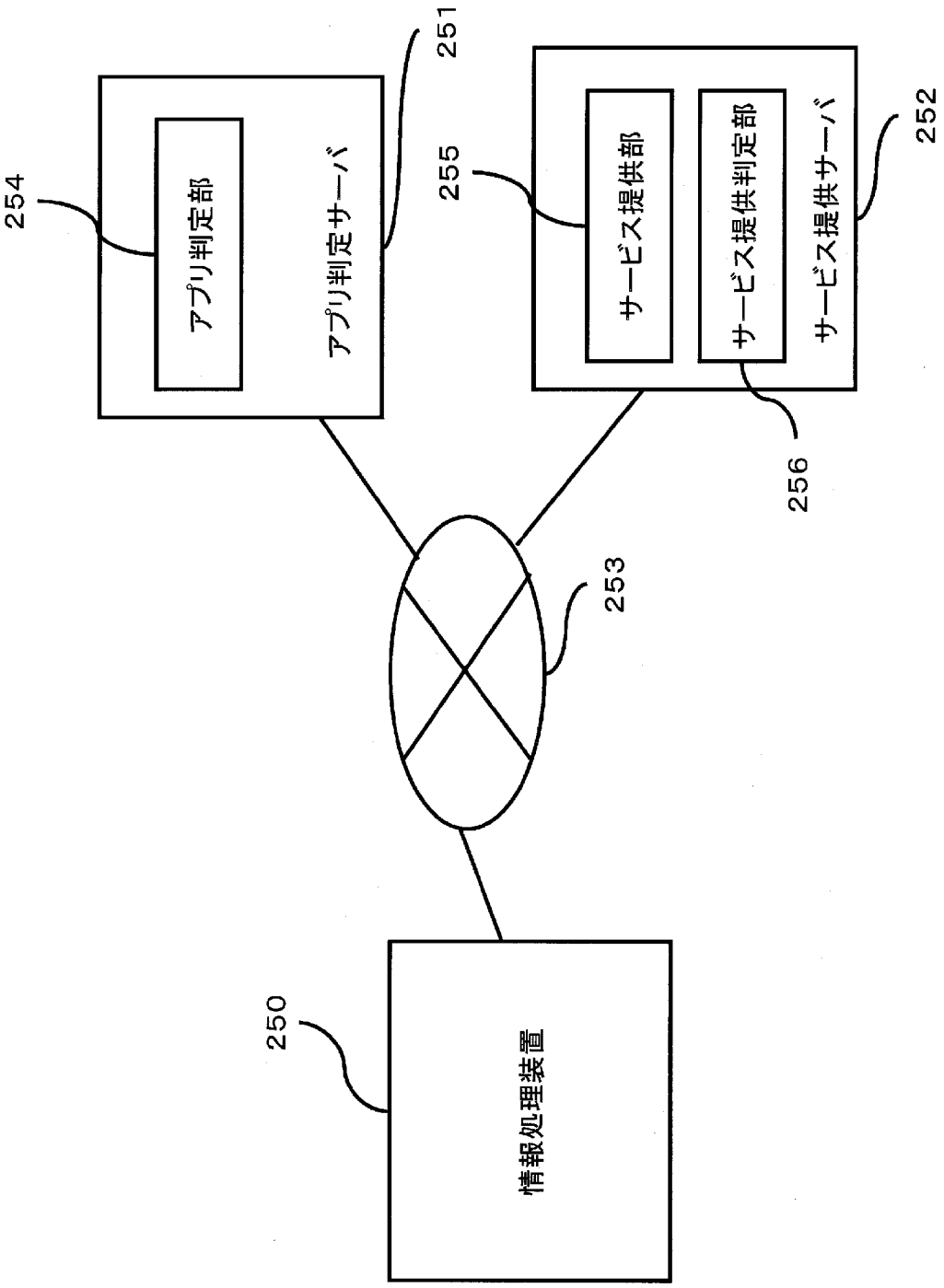
[図11]



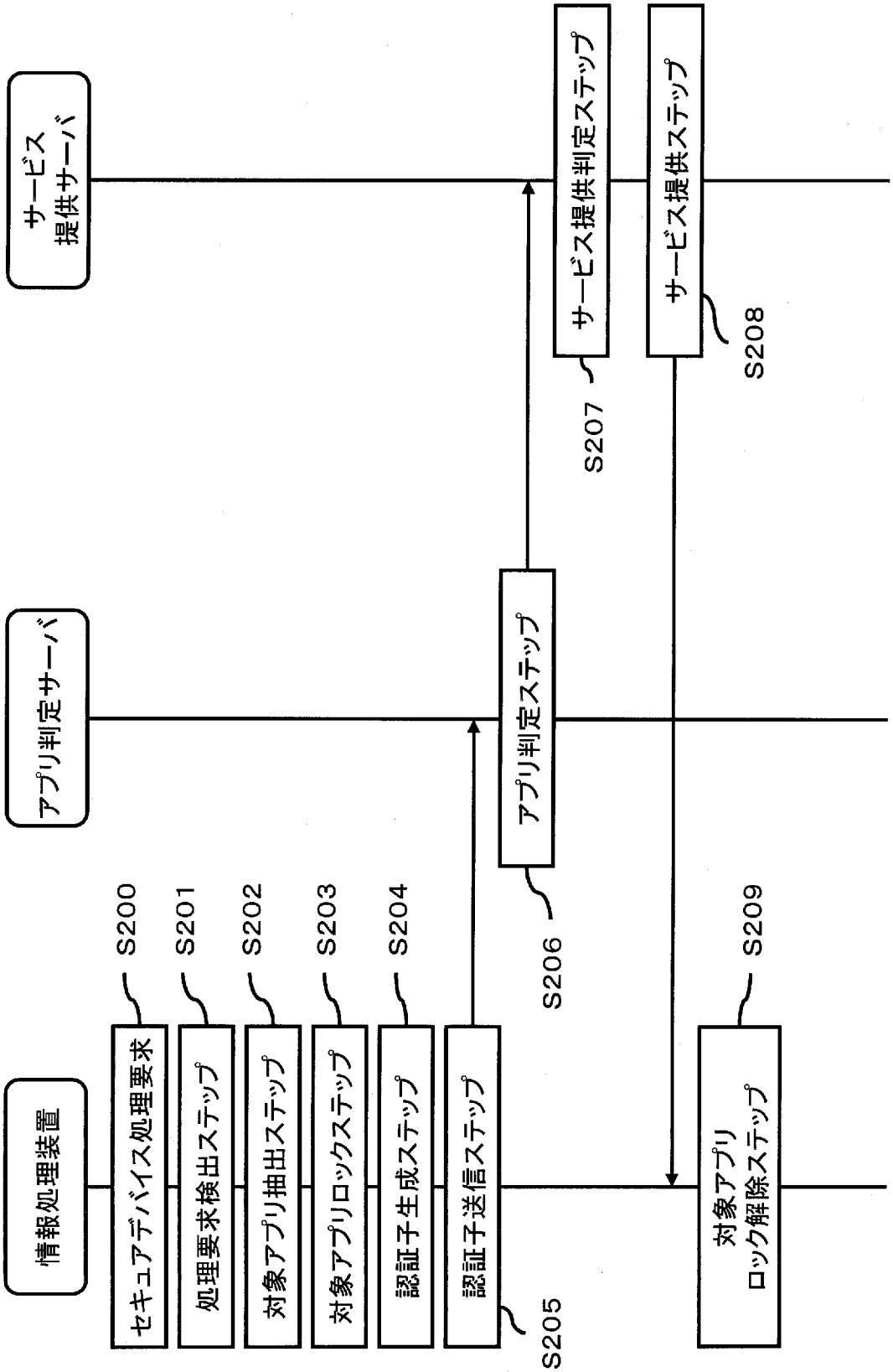
[図12]


240
241
234
236
認証子生成部
通信部
アプリ特定部
管理専用OS
セキュアVMM
239
デバイスアクセス
要求判定部
ネットワーク
インターフェース
ドライバ
238
235
動作アプリメモリロック部
230
233
アプリケーションB
汎用OS
232
アプリケーションA
動作アプリ格納メモリ特定部
237
231

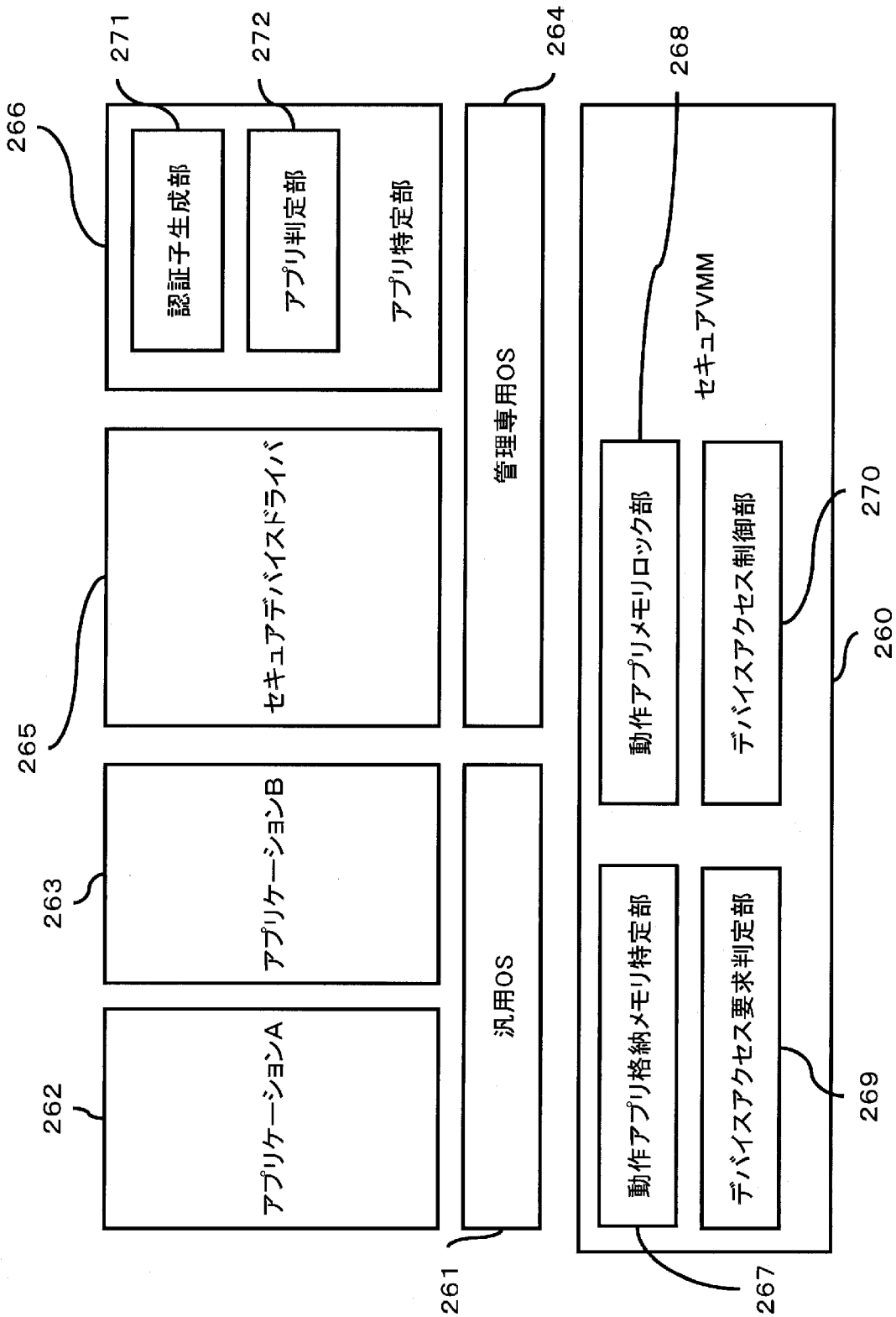
[図13]


250
情報処理装置
253
251
アプリ判定サーバ
254
アプリ判定部
252
サービス提供サーバ
255
サービス提供部
256
サービス提供判定部

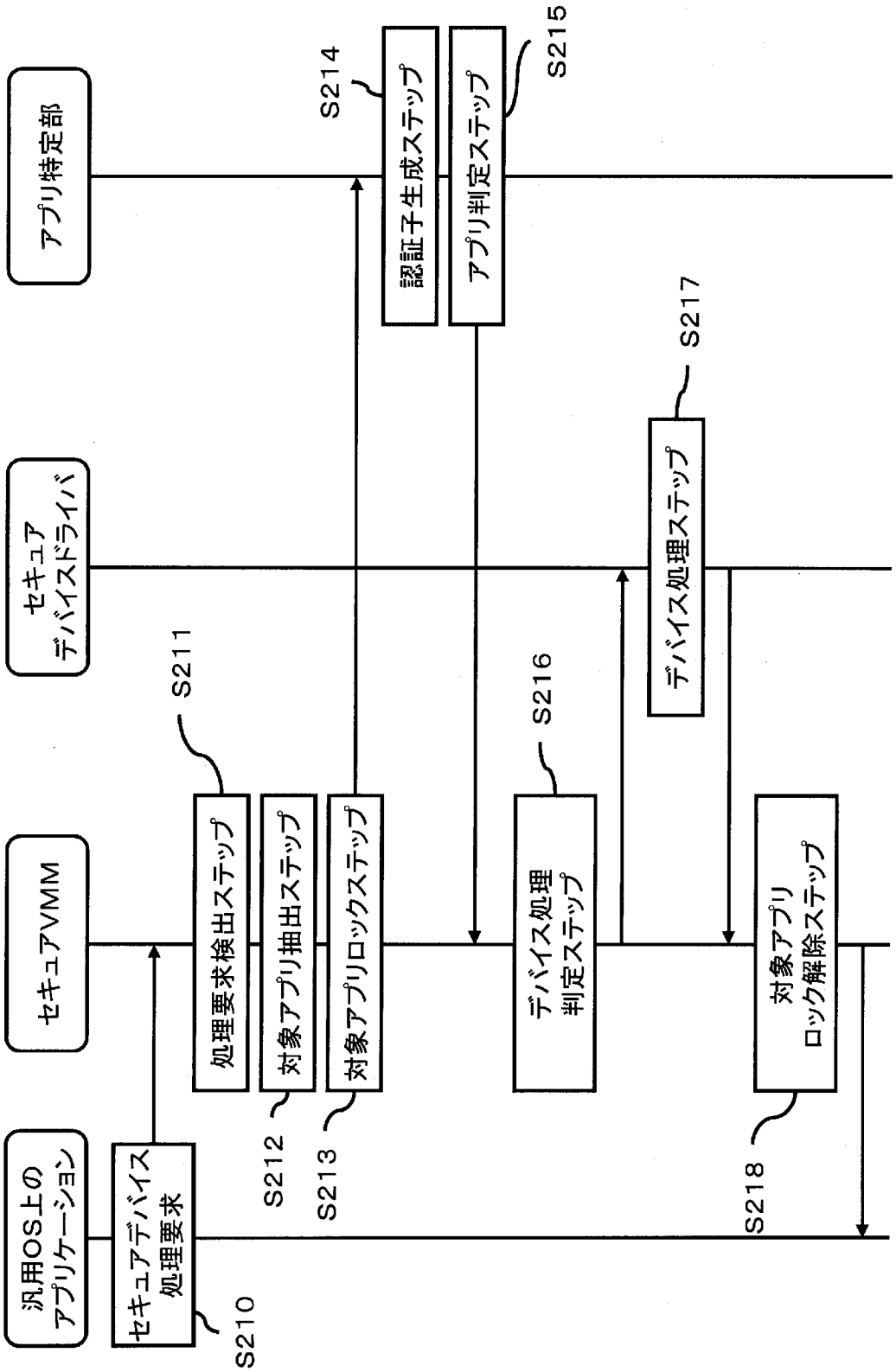
[図14]


情報処理装置
アプリ判定サーバ
サービス提供サーバ
セキュアデバイス処理要求
処理要求検出ステップ
対象アプリ抽出ステップ
対象アプリロックステップ
認証子生成ステップ
認証子送信ステップ
アプリ判定ステップ
サービス提供判定ステップ
サービス提供ステップ
対象アプリロック解除ステップ
S200
S201
S202
S203
S204
S205
S206
S207
S208
S209

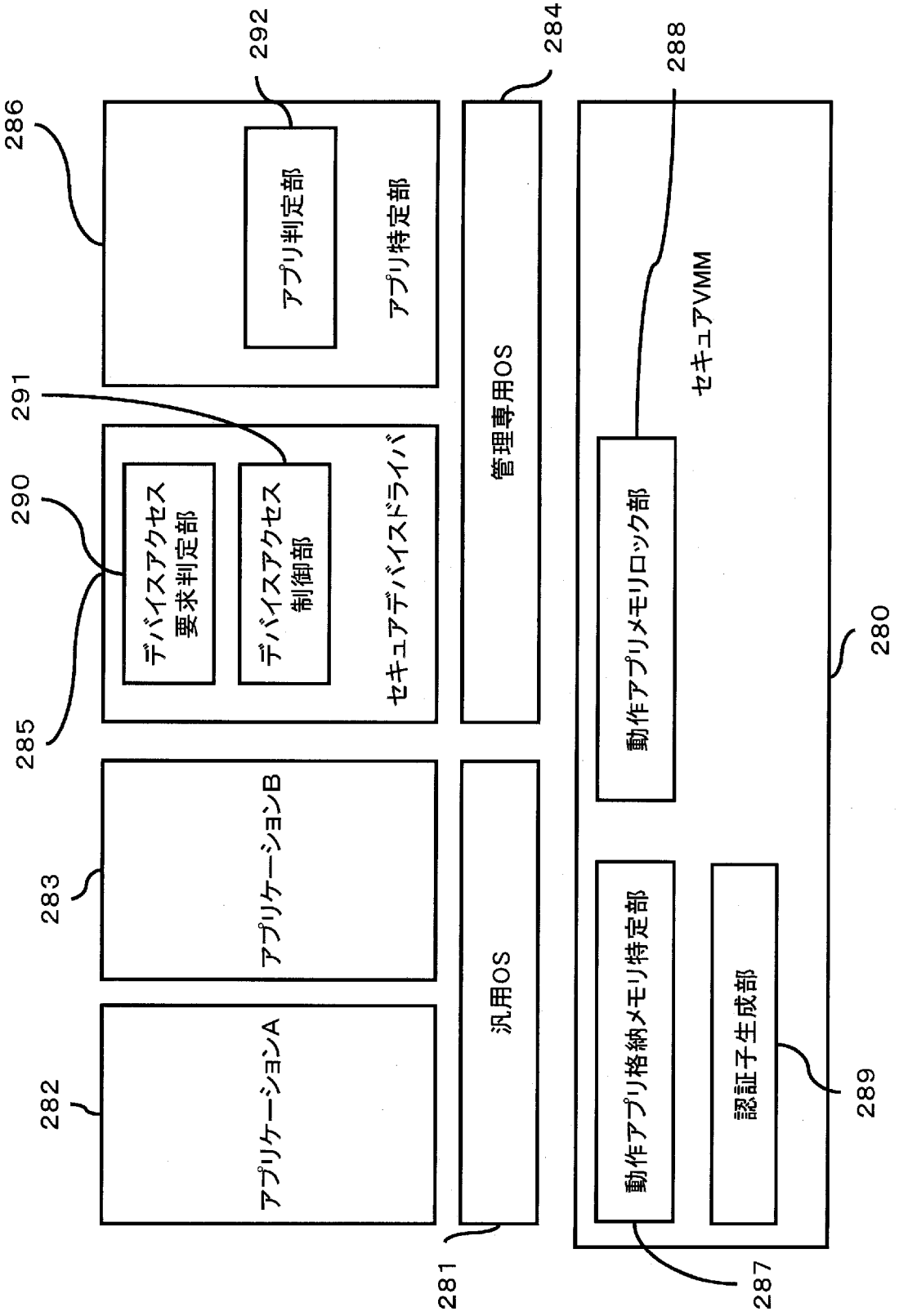
[図15]


271
272
264
268
266
認証子生成部
アプリ判定部
アプリ特定部
管理専用OS
セキュアVMM
セキュアデバイスドライバ
動作アプリメモリロック部
デバイスアクセス制御部
270
265
260
アプリケーションB
263
262
アプリケーションA
汎用OS
動作アプリ格納メモリ特定部
デバイスアクセス要求判定部
269
261
267

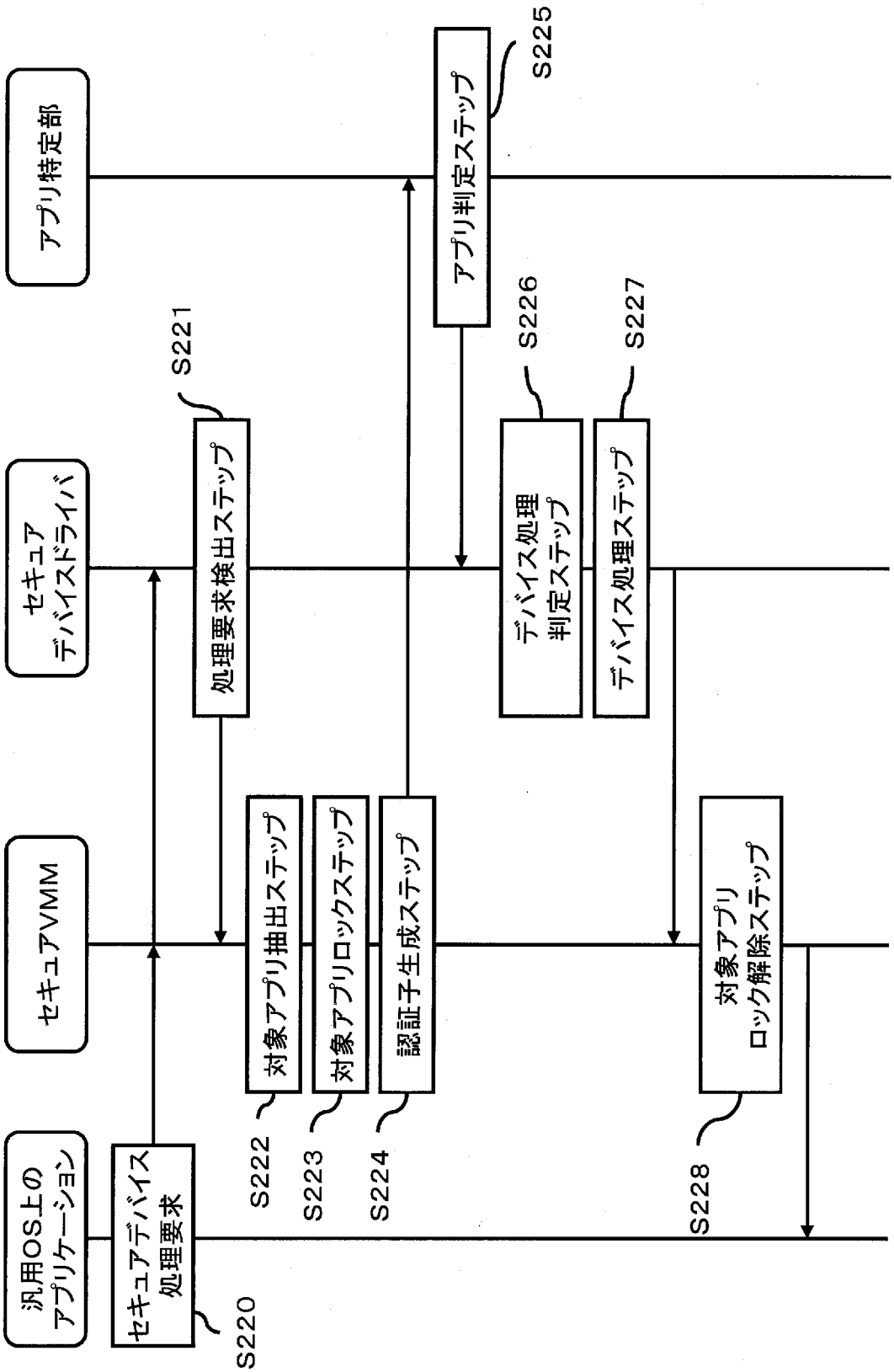
[図16]


汎用OS上のアプリケーション
セキュアVMM
セキュアデバイスドライバ
アプリ特定部
セキュアデバイス処理要求
S210
処理要求検出ステップ
S211
対象アプリ抽出ステップ
S212
対象アプリロックステップ
S213
認証子生成ステップ
S214
アプリ判定ステップ
S215
デバイス処理判定ステップ
S216
デバイス処理ステップ
S217
対象アプリロック解除ステップ
S218

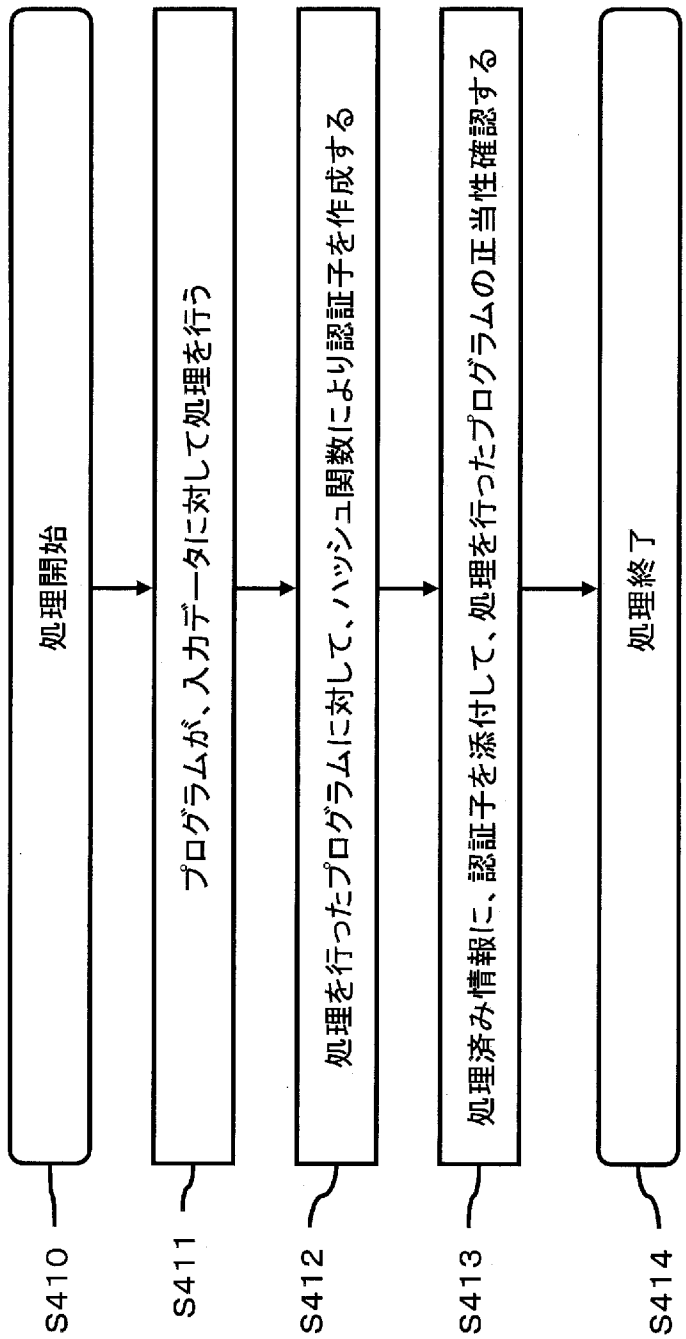
[図17]


280
281
282
283
284
285
286
287
288
289
290
291
292
アプリケーションA
アプリケーションB
汎用OS
管理専用OS
セキュアデバイスドライバ
デバイスアクセス要求判定部
デバイスアクセス制御部
アプリ特定部
アプリ判定部
セキュアVMM
動作アプリメモリロック部
動作アプリ格納メモリ特定部
認証子生成部

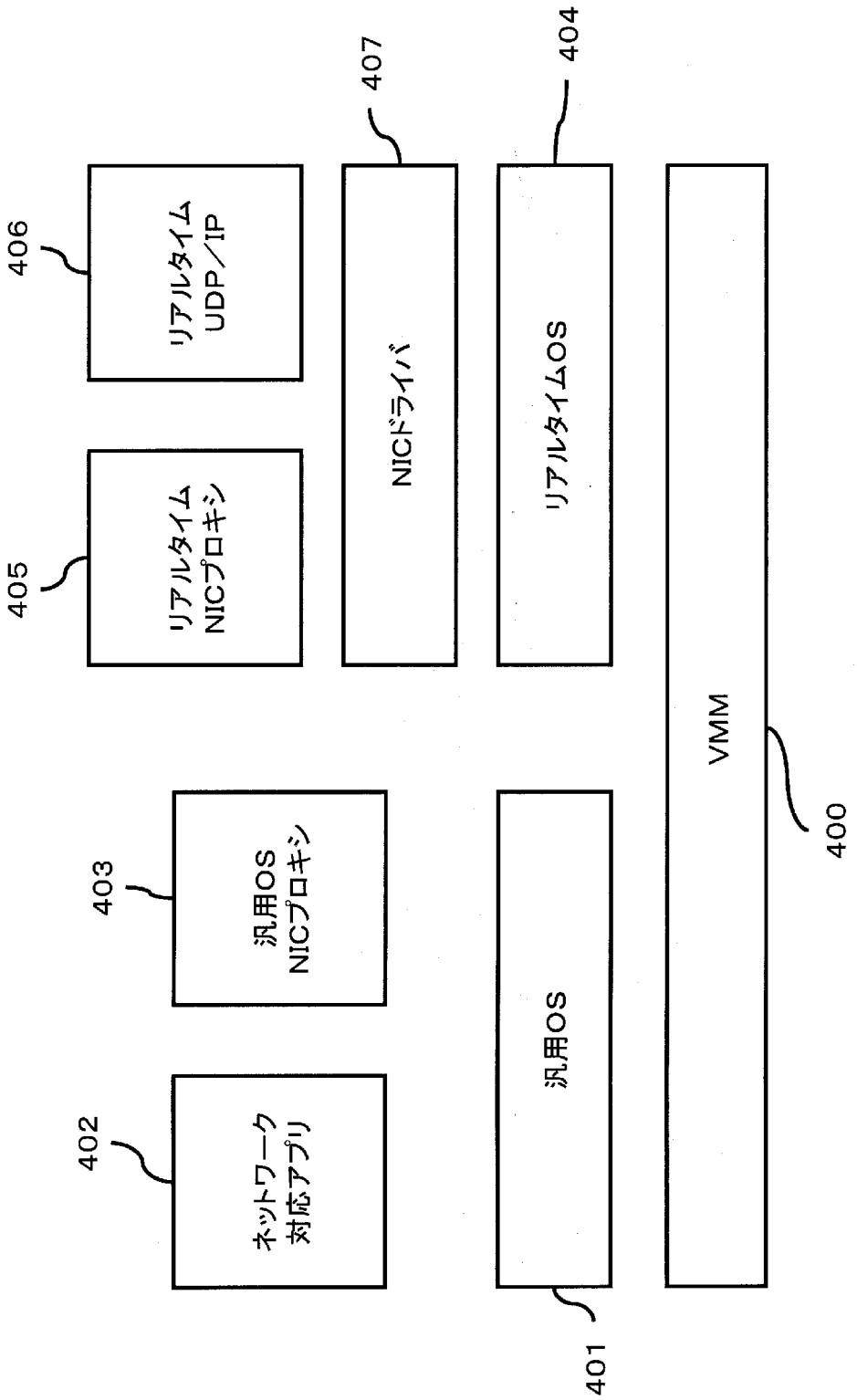
[図18]


汎用OS上の
アプリケーション
セキュアVMM
セキュア
デバイスドライバ
アプリ特定部
セキュアデバイス
処理要求
S220
対象アプリ抽出ステップ
S222
対象アプリロックステップ
S223
認証子生成ステップ
S224
処理要求検出ステップ
S221
アプリ判定ステップ
S225
デバイス処理
判定ステップ
S226
デバイス処理ステップ
S227
対象アプリ
ロック解除ステップ
S228

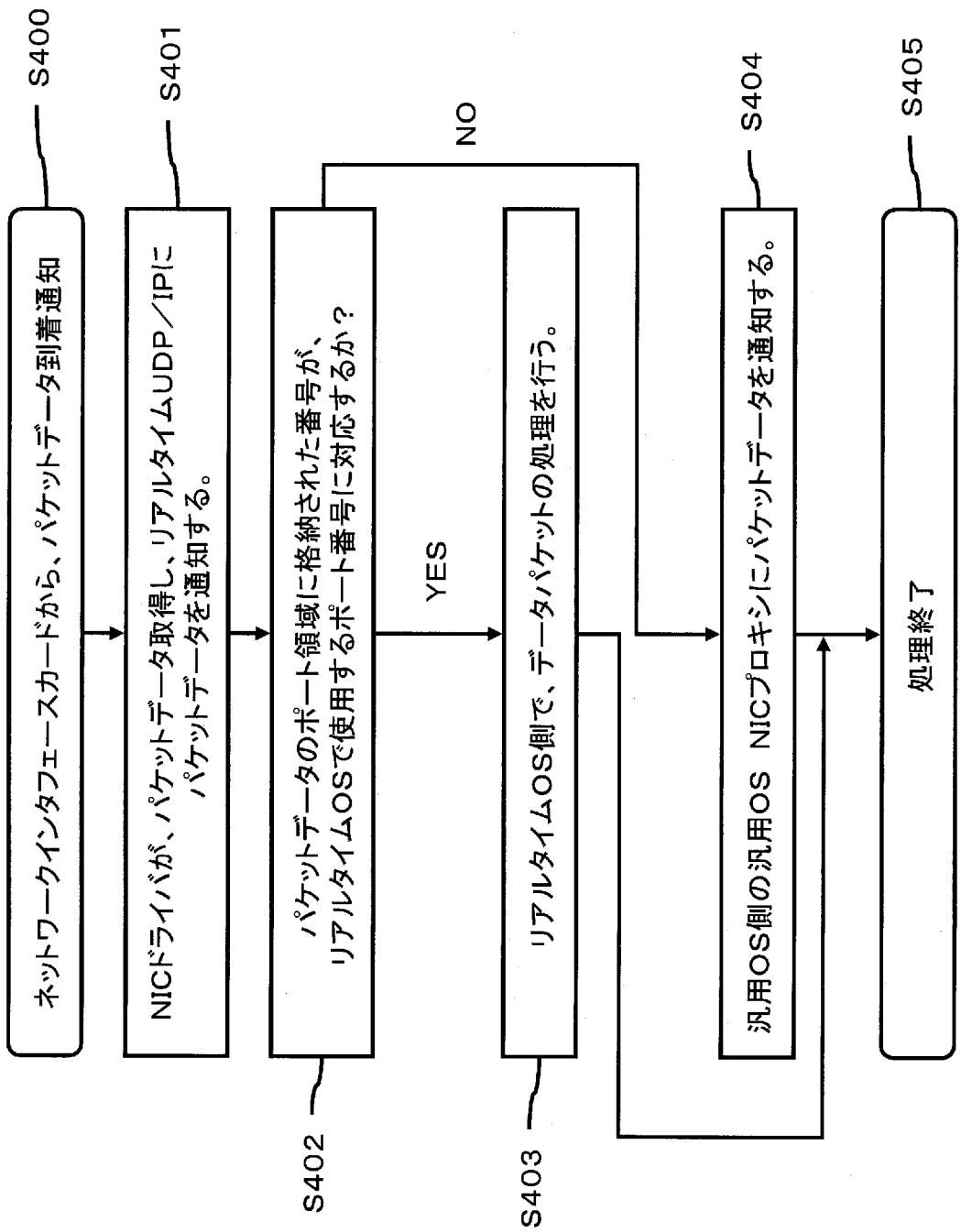
[図19]


処理開始
プログラムが、入力データに対して処理を行う
処理を行ったプログラムに対して、ハッシュ関数により認証子を作成する
処理済み情報に、認証子を添付して、処理を行ったプログラムの正当性確認する
処理終了
S410
S411
S412
S413
S414

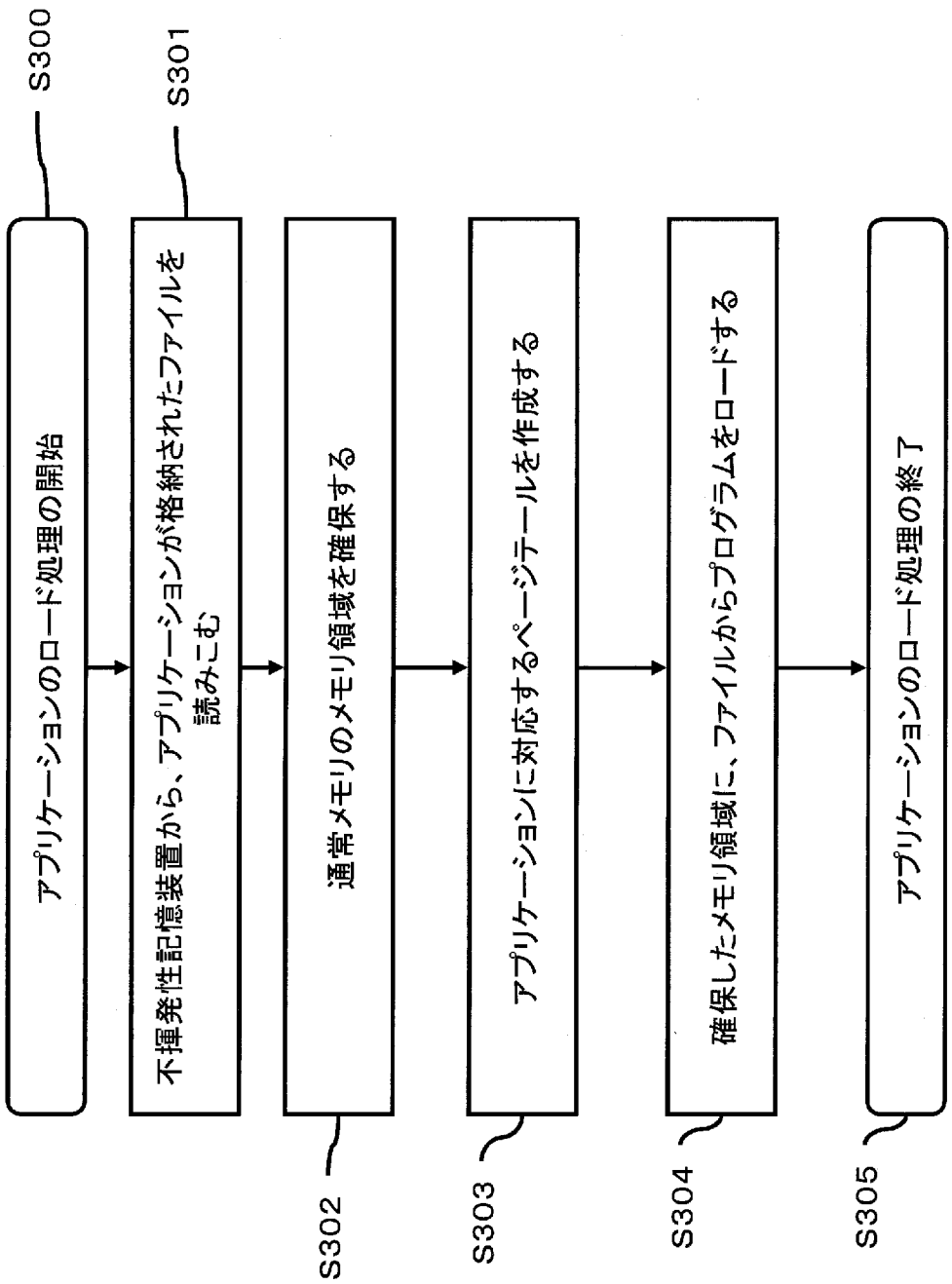
[図20]


406
リアルタイム
UDP／IP
405
リアルタイム
NICプロキシ
407
NICドライバ
404
リアルタイムOS
VMM
400
403
汎用OS
NICプロキシ
402
ネットワーク
対応アプリ
汎用OS
401

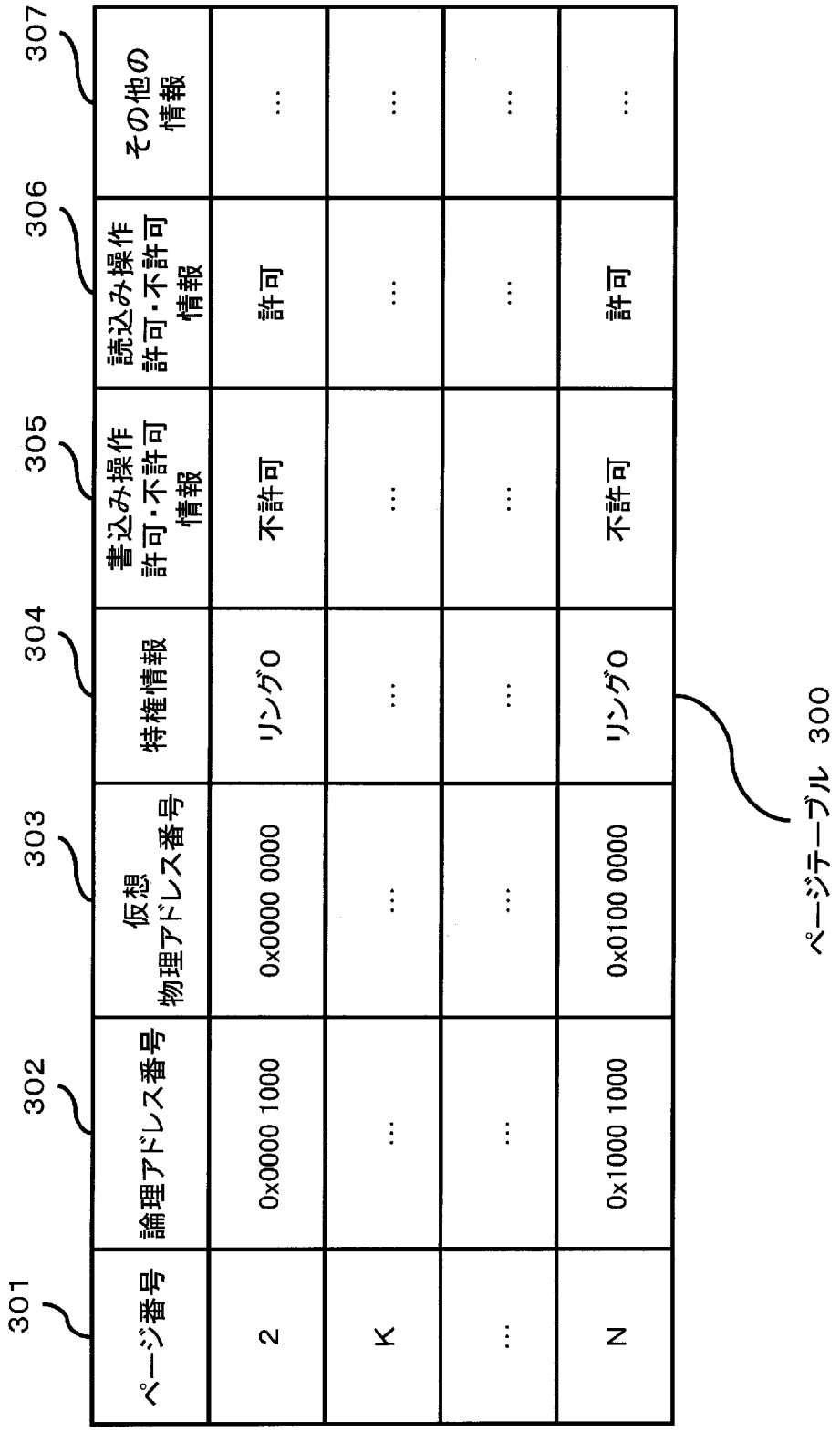
[図21]


S400
ネットワークインタフェースカードから、パケットデータ到着通知
S401
NICドライバが、パケットデータ取得し、リアルタイムUDP／IPにパケットデータを通知する。
S402
パケットデータのポート領域に格納された番号が、リアルタイムOSで使用するポート番号に対応するか？
YES
NO
S403
リアルタイムOS側で、データパケットの処理を行う。
S404
汎用OS側の汎用OS NICプロキシにパケットデータを通知する。
S405
処理終了

[図22]


S300
アプリケーションのロード処理の開始
S301
不揮発性記憶装置から、アプリケーションが格納されたファイルを読みこむ
S302
通常メモリのメモリ領域を確保する
S303
アプリケーションに対応するページテーブルを作成する
S304
確保したメモリ領域に、ファイルからプログラムをロードする
S305
アプリケーションのロード処理の終了

[図23]


301
302
303
304
305
306
307
ページ番号
論理アドレス番号
仮想
物理アドレス番号
特権情報
書込み操作
許可・不許可
情報
読込み操作
許可・不許可
情報
その他の
情報
2
0x0000 1000
0x0000 0000
リング0
不許可
許可
…
K
…
…
…
…
…
…
…
…
…
…
…
…
…
…
…
N
0x1000 1000
0x0100 0000
リング0
不許可
許可
…
ページテーブル 300

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/000500

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/22(2006.01)i, *G06F12/14*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/22, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2009
Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-337864 A (Hitachi, Ltd.), 07 December, 2001 (07.12.01), Par. Nos. [0026] to [0027], [0031], [0046] to [0056]; Figs. 1, 4, 7 to 9 & US 2001/0025311 A1	1-12
Y	JP 2006-065847 A (Microsoft Corp.), 09 March, 2006 (09.03.06), Par. Nos. [0039], [0045], [0052] to [0056]; Figs. 7 to 8 & US 2006/0047958 A1 & EP 1638031 A1 & CN 1740941 A	1-12
A	JP 2001-175486 A (Hitachi, Ltd.), 29 June, 2001 (29.06.01), Abstract (Family: none)	1,8-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 March, 2009 (12.03.09)	24 March, 2009 (24.03.09)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／０００５００

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/22(2006.01)i, G06F12/14(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/22, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2001-337864 A (株式会社日立製作所) 2001.12.07, 第26-27,31,46-56段落,図1,4,7-9 & US 2001/0025311 A1	1-12
Y	JP 2006-065847 A (マイクロソフトコーポレーション) 2006.03.09, 第39,45,52-56段落,図7-8 & US 2006/0047958 A1 & EP 1638031 A1 & CN 1740941 A	1-12
A	JP 2001-175486 A (株式会社日立製作所) 2001.06.29, 【要約】 (ファミリーなし)	1,8-12

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 １２．０３．２００９	国際調査報告の発送日 ２４．０３．２００９
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　９０７１ 平井　誠 電話番号　０３－３５８１－１１０１　内線　３５４６